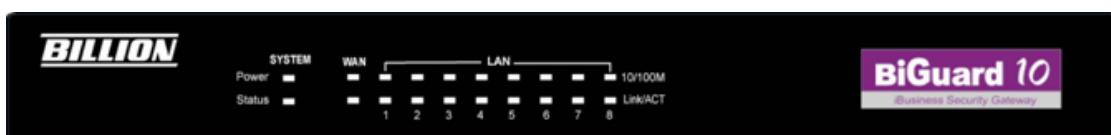


BiGuard 10

iBusiness Security Gateway Small-Office



BiGuard 2

iBusiness Security Gateway Home-Office



User's Manual

Version Release 4.00 (FW:1.05)

BiGuard 2/10 User's Manual

(Updated June 1, 2006)

Copyright Information

© 2006 Billion Electric Corporation, Ltd.

The contents of this publication may not be reproduced in whole or in part, transcribed, stored, translated, or transmitted in any form or any means, without the prior written consent of Billion Electric Corporation.

Published by Billion Electric Corporation. All rights reserved.

Disclaimer

Billion does not assume any liability arising out of the application of use of any products or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Billion reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Mac OS is a registered trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP are registered trademarks of Microsoft Corporation.

Safety Warnings



Your BiGuard 2/10 is built for reliability and long service life. For your safety, be sure to read and follow the following safety warnings.

- Read this installation guide thoroughly before attempting to set up your BiGuard 2/10.
- Your BiGuard 2/10 is a complex electronic device. DO NOT open or attempt to repair it yourself. Opening or removing the covers can expose you to high voltage and other risks. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
- Connect the power cord to the correct supply voltage.
- Carefully place connecting cables to avoid people from stepping or tripping on them. DO NOT allow anything to rest on the power cord and DO NOT place the power cord in an area where it can be stepped on.
- DO NOT use BiGuard 2/10 in environments with high humidity or high temperatures.
- DO NOT use the same power source for BiGuard 2/10 as other equipment.
- DO NOT use your BiGuard 2/10 and any accessories outdoors.
- If you mount your BiGuard 2/10, make sure that no electrical, water or gas pipes will be damaged during installation.
- DO NOT install or use your BiGuard 2/10 during a thunderstorm.
- DO NOT expose your BiGuard 2/10 to dampness, dust, or corrosive liquids.
- DO NOT use your BiGuard 2/10 near water.
- Be sure to connect the cables to the correct ports.
- DO NOT obstruct the ventilation slots on your BiGuard 2/10 or expose it to direct sunlight or other heat sources. Excessive temperatures may damage your device.
- DO NOT store anything on top of your BiGuard 2/10.
- Only connect suitable accessories to your BiGuard 2/10.
- Keep packaging out of the reach of children.
- If disposing of the device, please follow your local regulations for the safe disposal of electronic products to protect the environment.

Table of Contents

Chapter 1: Introduction

- 1.1 Overview**
- 1.2 Product Highlights**
 - 1.2.1 Virtual Private Network Support**
 - 1.2.2 Advanced Firewall Security**
 - 1.2.3 Intelligent Bandwidth Management**
- 1.3 Package Contents**
 - 1.3.1 BiGuard 10**
 - 1.3.1.1 Front Panel**
 - 1.3.1.2 Rear Panel**
 - 1.3.1.3 Rack Mounting**
 - 1.3.1.4 Cabling**
 - 1.3.2 BiGuard 2**
 - 1.3.2.1 Front Panel**
 - 1.3.2.2 Rear Panel**
 - 1.3.2.3 Cabling**

Chapter 2: Router Applications

- 2.1 Overview**
- 2.2 Bandwidth Management with QoS**
 - 2.2.1 QoS Technology**
 - 2.2.2 QoS Policies for Different Applications**
 - 2.2.3 Guaranteed / Maximum Bandwidth**
 - 2.2.4 Policy Based Traffic Shaping**
 - 2.2.5 Priority Bandwidth Utilization**
 - 2.2.6 Management by IP or MAC address**
 - 2.2.7 DiffServ (DSCP Marking)**
- 2.3 Virtual Private Networking**
 - 2.3.1 General VPN Setup**
 - 2.3.2 Concentrator**

Chapter 3: Getting Started

- 3.1 Overview**
- 3.2 Before You Begin**
- 3.3 Connecting Your Router**
- 3.4 Configuring PCs for TCP/IP Networking**
 - 3.4.1 Overview**
 - 3.4.2 Windows XP**
 - 3.4.2.1 Configuring**
 - 3.4.2.2 Verifying Settings**
 - 3.4.3 Windows 2000**
 - 3.4.3.1 Configuring**
 - 3.4.3.2 Verifying Settings**
 - 3.4.4 Windows 98 / ME**
 - 3.4.4.1 Installing Components**
 - 3.4.4.2 Configuring**
 - 3.4.4.3 Verifying Settings**
- 3.5 Factory Default Settings**
 - 3.5.1 Username and Password**
 - 3.5.2 LAN and WAN Port Addresses**
- 3.6 Information From Your ISP**
 - 3.6.1 Protocols**
 - 3.6.2 Configuration Information**
- 3.7 Web Configuration Interface**

Chapter 4: Router Configuration

- 4.1 Overview**
- 4.2 Status**
 - 4.2.1 ARP Table**
 - 4.2.2 Routing Table**
 - 4.2.3 Session Table**
 - 4.2.4 DHCP Table**
 - 4.2.5 IPSec Status**
 - 4.2.6 PPTP Status**
 - 4.2.7 System Log**
 - 4.2.8 IPSec Log**
- 4.3 Quick Start**
 - 4.3.1 DHCP**
 - 4.3.2 Static IP**
 - 4.3.3 PPPoE**
 - 4.3.4 PPTP**
 - 4.3.5 Big Pond**
- 4.4 Configuration**
 - 4.4.1 LAN**
 - 4.4.1.1 Ethernet**
 - 4.4.1.2 DHCP Server**
 - 4.4.1.3 LAN Address Mapping**
 - 4.4.2 WAN**
 - 4.4.2.1 WAN**
 - 4.4.2.1.1 DHCP
 - 4.4.2.1.2 Static IP
 - 4.4.2.1.3 PPPoE
 - 4.4.2.1.4 PPTP
 - 4.4.2.1.5 Big Pond
 - 4.4.2.2 Bandwidth Settings**
 - 4.4.2.3 WAN IP Alias**
 - 4.4.3 System**
 - 4.4.3.1 Time Zone**
 - 4.4.3.2 Remote Access**
 - 4.4.3.3 Firmware Upgrade**
 - 4.4.3.4 Backup / Restore**
 - 4.4.3.5 Restart**
 - 4.4.3.6 Password**

- 4.4.3.7 System Log Server
- 4.4.3.8 E-mail Alert
- 4.4.4 Firewall
 - 4.4.4.1 Packet Filter
 - 4.4.4.2 URL Filter
 - 4.4.4.3 LAN MAC Filter
 - 4.4.4.4 Block WAN Request
 - 4.4.4.5 Intrusion Detection
- 4.4.5 VPN
 - 4.4.5.1 IPSec
 - 4.4.5.1.1 IPSec Wizard
 - 4.4.5.1.2 IPSec Policy
 - 4.4.5.2 PPTP
- 4.4.6 QoS
- 4.4.7 Virtual Server
 - 4.4.7.1 DMZ
 - 4.4.7.2 Port Forwarding
- 4.4.8 Advanced
 - 4.4.8.1 Static Route
 - 4.4.8.2 Dynamic DNS
 - 4.4.8.3 Device Management
 - 4.4.8.4 IGMP
 - 4.4.8.5 VLAN Bridge
- 4.5 Save Configuration To Flash
- 4.6 Logout

Chapter 5: Troubleshooting

- 5.1 Basic Functionality
 - 5.1.1 Router Won't Turn On
 - 5.1.2 LEDs Never Turn Off
 - 5.1.3 LAN or Internet Port Not On
 - 5.1.4 Forgot My Password
- 5.2 LAN Interface
 - 5.2.1 Can't Access BiGuard 2/10 from the LAN
 - 5.2.2 Can't Ping Any PC on the LAN
 - 5.2.3 Can't Access Web Configuration Interface
 - 5.2.3.1 Pop-up Windows

5.2.3.2 Javascripts

5.2.3.3 Java Permissions

5.3 WAN Interface

5.3.1 Can't Get WAN IP Address from the ISP

5.4 ISP Connection

5.5 Problems with Date and Time

5.6 Restoring Factory Defaults

Appendix A: Product Specifications

A.1 BiGuard 10 Product Specifications

A.2 BiGuard 2 Product Specifications

Appendix B: Customer Support

Appendix C: FCC Interference Statement

Appendix D: Network, Routing, and Firewall Basics

D.1 Network Basics

D.1.1 IP Addresses

D.1.1.1 Netmask

D.1.1.2 Subnet Addressing

D.1.1.3 Private IP Addresses

D.1.2 Network Address Translation (NAT)

D.1.3 Dynamic Host Configuration Protocol (DHCP)

D.2 Router Basics

D.2.1 What is a Router?

D.2.2 Why use a Router?

D.2.3 Routing Information Protocol (RIP)

D.3 Firewall Basics

D.3.1 What is a Firewall?

D.3.1.1 Stateful Packet Inspection

D.3.1.2 Denial of Service (DoS) Attack

D.3.2 Why Use a Firewall?

Appendix E: Virtual Private Networking

- E.1 What is a VPN?
 - E.1.1 VPN Applications
- E.2 What is IPsec?
 - E.2.1 IPsec Security Components
 - E.2.1.1 Authentication Header (AH)
 - E.2.1.2 Encapsulating Security Payload (ESP)
 - E.2.1.3 Security Associations (SA)
 - E.2.2 IPsec Modes
 - E.2.3 Tunnel Mode AH
 - E.2.4 Tunnel Mode ESP
 - E.2.5 Internet Key Exchange (IKE)

Appendix F: IPsec Logs and Events

- F.1 IPsec Log Event Categories
- F.2 IPsec Log Event Table

Appendix G: Bandwidth Management with QoS

- G.1 Overview
- G.2 What is Quality of Service?
- G.3 How Does QoS Work?
- G.4 Who Needs QoS?
 - G.4.1 Home Users
 - G.4.2 Office Users

Appendix H: Router Setup Examples

- H.1 VPN Configuration
 - H.1.1 LAN to LAN
 - H.1.2 Host to LAN
- H.2 VPN Concentrator
- H.3 Intrusion Detection
- H.4 PPTP Remote Access by Windows XP
- H.5 PPTP Remote Access by BiGuard

Chapter 1: Introduction

1.1 Overview

Congratulations on purchasing BiGuard 2/10 Router from Billion. Combining a router with an Ethernet network switch, BiGuard 2/10 is a state-of-the-art device that provides everything you need to get your network connected to the Internet over your Cable or DSL connection quickly and easily. The Quick Start Wizard and DHCP Server will get first-time users up and running with minimal fuss and configuration, while sophisticated Quality of Service (QoS) and traffic management features grant advanced users total control over their network and Internet connection.

This manual illustrates the many features and functions of BiGuard 2/10, and even takes you through the various ways you can apply this versatile device to your home or office. Take the time now to familiarize yourself with BiGuard 2/10.

1.2 Product Highlights

1.2.1 Virtual Private Network Support

BiGuard 2/10 supports comprehensive IPSec VPN protocols for businesses to establish private encrypted tunnels over the Internet to ensure data transmission security among multiple sites, such as a branch office or dial-up connection. Up to 2/10 simultaneous IPSec VPN connections are possible on BiGuard 2/10, with performance of up to 4/20 Mbps.

1.2.2 Advanced Firewall Security

Aside from intelligent broadband sharing, BiGuard 2/10 offers integrated firewall protection with advanced features to secure your network from outside attacks. Stateful Packet Inspection (SPI) determines if a data packet is permitted to enter the private LAN. Denial of Service (DoS) prevents hackers from interrupting network services via malicious attacks. In addition, BiGuard 2/10 firewall can be configured to alert you via email should your network come under fire, offering both tight network security and peace of mind.

1.2.3 Intelligent Bandwidth Management

BiGuard 2/10 utilizes Quality of Service (QoS) to give you full control over the priority of both incoming and outgoing data, ensuring that critical data such as customer information moves through your network, even while under a heavy load. Transmission speeds can be throttled to make sure users are not saturating bandwidth required for mission-critical data transfers. Priority types of upload data can also be changed, allowing BiGuard 2/10 to automatically sort out actual speeds for unmatched convenience.

1.3 Package Contents

1.3.1 BiGuard 10

- BiGuard 10 iBusiness Security Gateway Small-Office
- Bracket x 2 (for rack-mounting)
- Screw x 4 (for rack-mounting)
- Getting Started CD-ROM
- Quick Start Guide
- AC-DC Power Adapter (12VDC, 1A)

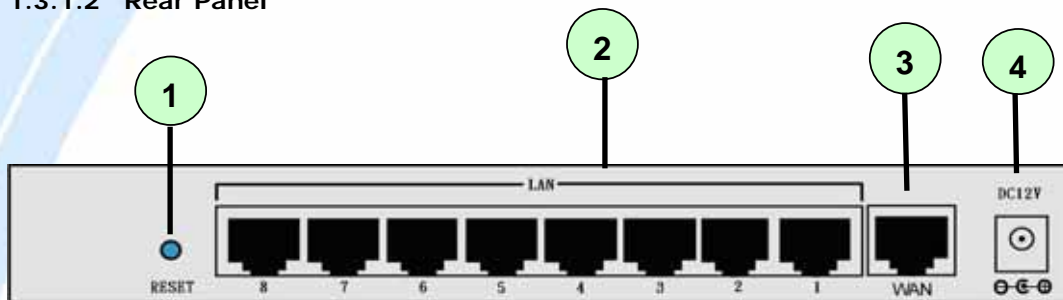
1.3.1.1 Front Panel



LED	Function
Power	A solid light indicates a steady connection to a power source.
Status	A blinking light indicates the device is writing to flash memory.
WAN	Lit when connected to an Ethernet device. 10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps.

	Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.
LAN 1 – 8	Lit when connected to an Ethernet device. 10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps. Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.

1.3.1.2 Rear Panel



Port	Meaning
1	RESET After the device is powered on, press it to reset the device or restore to factory default settings. 0-3 seconds: The Status LED will light 6 seconds above: restore to factory default settings (this is used when you cannot login to the router. E.g. forgot the password)
2	LAN 1X – 8X (RJ-45 connector) Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the eight LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
3	WAN WAN 10/100M Ethernet port (with auto crossover support); connect xDSL/Cable modem here.
4	DC12V Connect DC power adapter here.(DC12V Power)

1.3.1.3 Rack Mounting

To rack mount BiGuard 10, carefully secure the device to your rack on both sides using the included brackets and screws. See the diagram below for a more detailed explanation.



1.3.1.4 Cabling

Most Ethernet networks currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector.

One of the most common causes of networking problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of BiGuard 10, verify that the LAN link and WAN line LEDs are lit. If they are not, check to see that you are using the proper cabling.

1.3.2 BiGuard 2

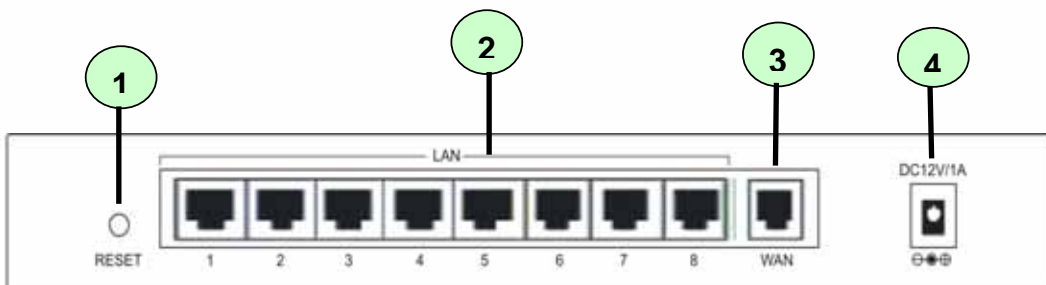
BiGuard 2 iBusiness Security Gateway Home-Office
Getting Started CD-ROM
Quick Start Guide
Ethernet (CAT-5 LAN) Cable
AC-DC Power Adapter (12VDC, 1A)

1.3.2.1 Front Panel



LED	Function
POWER	A solid light indicates a steady connection to a power source.
STATUS	A blinking light indicates the device is writing to flash memory.
WAN	<p>Lit when connected to an Ethernet device.</p> <p>10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps.</p> <p>Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.</p>
LAN 1 - 8	<p>Lit when connected to an Ethernet device.</p> <p>10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps.</p> <p>Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.</p>

1.3.2.2 Rear Panel



Port		Meaning
1	RESET	After the device is powered on, press it to reset the device or restore to factory default settings. 0-3 seconds: The Status LED will light 6 seconds above: restore to factory default settings (this is used when you cannot login to the router. E.g. forgot the password)
2	LAN 1X — 8X (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the eight LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
3	WAN	WAN 10/100M Ethernet port (with auto crossover support); connect xDSL/Cable modem here.
4	DC12V	Connect DC power adapter here.(DC12V Power)

1.3.2.3 Cabling

Most Ethernet networks currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector.

One of the most common causes of networking problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of BiGuard 2, verify that the LAN link and WAN line LEDs are lit. If they are not, check to see that you are using the proper cabling.

Chapter 2: Router Applications

2.1 Overview

Your BiGuard 2/10 Router is a versatile device that can be configured to not only protect your network from malicious attackers, but also ensure optimal usage of available bandwidth with Quality of Service (QoS). Alternatively, BiGuard 2/10 can also be set to handle secure connections with Virtual Private Networking (VPN).

The following chapter describes how BiGuard 2/10 can work for you.

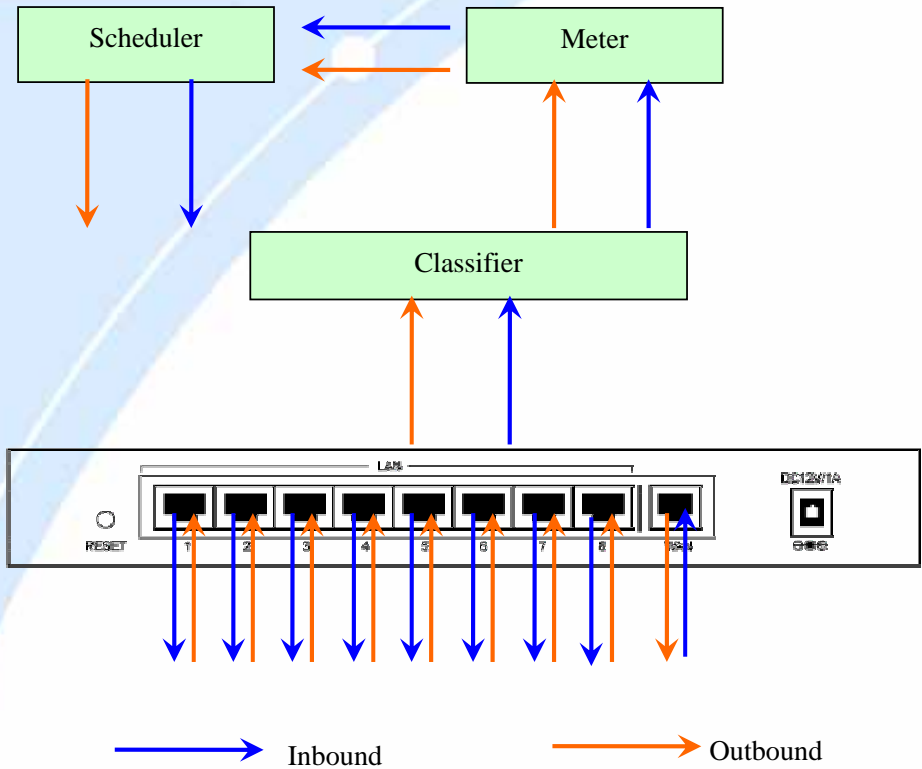
2.2 Bandwidth Management with QoS

Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router. By doing so, the router can ensure that latency-sensitive applications like voice, bandwidth-consuming data like gaming packets, or even mission critical files efficiently move through the router even under a heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

2.2.1 QoS Technology

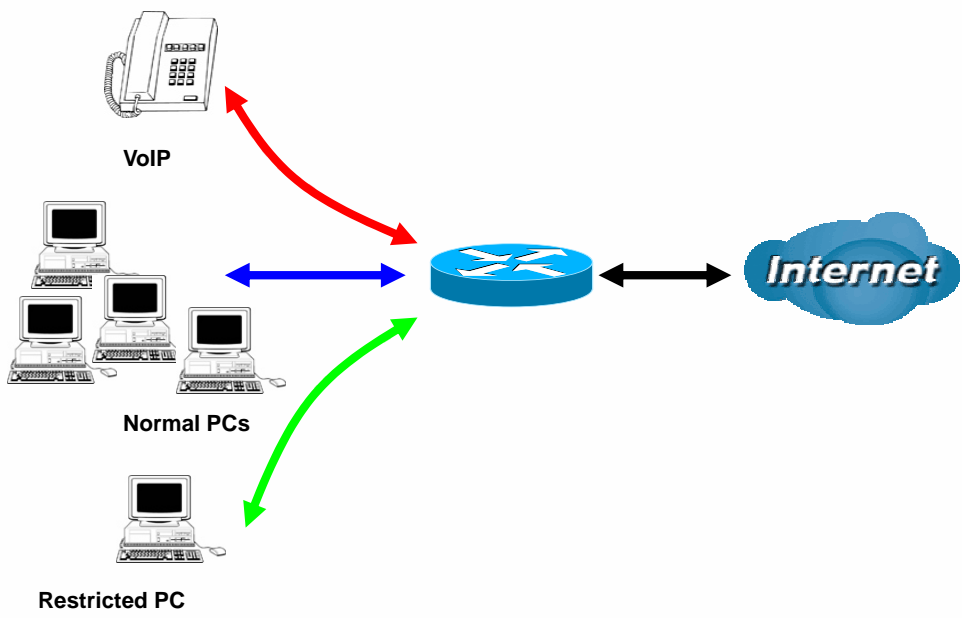
QoS generally involves the prioritization of network traffic. QoS is comprised of three major components: Classifier, Meter, and Scheduler. Each of these components has a distinct role in ensuring that incoming and outgoing data is managed according to user specifications.

The Classifier analyses incoming packets and marks each one according to configured parameters. The Meter communicates the drop priority to the Scheduler and measures the temporal priorities of the output stream against configured parameters. Finally, the Scheduler schedules each packet for transmission based on information from both the Classifier and the Meter.



2.2.2 QoS Policies for Different Applications

By setting different QoS policies according to the applications you are running, you can use BiGuard 2/10 to optimize the bandwidth that is being used on your network.



As illustrated in the diagram above, applications such as Voiceover IP (VoIP) require low network latencies to function properly. If bandwidth is being used by other applications such as an FTP server, users using VoIP will experience network lag and/or service interruptions during use. To avoid this scenario, this network has assigned VoIP with a guaranteed bandwidth and higher priority to ensure smooth communications. The FTP server, on the other hand, has been given a maximum bandwidth cap to make sure that regular service to both VoIP and normal Internet applications is uninterrupted.

2.2.3 Guaranteed / Maximum Bandwidth

Setting a Guaranteed Bandwidth ensures that a particular service receives a minimum percentage of bandwidth. For example, you can configure BiGuard 2/10 to reserve 10% of the available bandwidth for a particular computer on the network to transfer files.

Alternatively you can set a Maximum Bandwidth to restrict a particular application to a fixed percentage of the total throughput. Setting a Maximum Bandwidth of 20% for a file sharing program will ensure that no more than 20% of the available bandwidth will be used for file sharing.

Quality of Service		
Add QoS Rule		
Interface	WAN Outbound	
Application	FTP	
Packet Type	TCP	
Guaranteed	10	%
Maximum	20	%
Priority	6 (Lowest)	
DSCP Marking	Disabled	
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address	
Source IP Address Range	From 192.168.100.1	To 192.168.100.100
Destination IP Address Range	From 0.0.0.0	To 255.255.255.255
Source Port Range	From 1	To 65535
Destination Port Range	From 20	To 21
<input type="button" value="Apply"/>		

2.2.4 Policy Based Traffic Shaping

Policy Based Traffic Shaping allows you to apply specific traffic policies across a range of IP addresses or ports. This is particularly useful for assigning different policies for different PCs on the network. Policy based traffic shaping lets you better manage your bandwidth, providing reliable Internet and network service to your organization.

Quality of Service	
Add QoS Rule	
Interface	WAN Outbound
Application	FTP
Packet Type	TCP
Guaranteed	10 %
Maximum	20 %
Priority	6 (Lowest)
DSCP Marking	Disabled
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address
Source IP Address Range	From 192.168.100.1 To 192.168.100.100
Destination IP Address Range	From 0.0.0.0 To 255.255.255.255
Source Port Range	From 1 To 65535
Destination Port Range	From 20 To 21
<input type="button" value="Apply"/>	

2.2.5 Priority Bandwidth Utilization

Assigning priority to a certain service allows BiGuard 2/10 to give either a higher or lower priority to traffic from this particular service. Assigning a higher priority to an application ensures that it is processed ahead of applications with a lower priority and vice versa.

Quality of Service

Add QoS Rule

Interface	WAN Outbound		
Application	FTP		
Packet Type	TCP		
Guaranteed	1	%	
Maximum	5	%	
Priority	3 (Normal)		
DSCP Marking	<input type="checkbox"/> 0 (Highest) <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 (Normal) <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 (Lowest)		
Address Type	<input type="radio"/> IP Address <input checked="" type="radio"/> MAC Address		
Source IP Address Range	100/1	To	192.168.100.100
Destination IP Address Range		To	255.255.255.255
Source Port Range		To	65535
Destination Port Range	From 20	To	21

Apply

2.2.6 Management by IP or MAC address

BiGuard 2/10 can also be configured to apply traffic policies based on a particular IP or MAC address. This allows you to quickly assign different traffic policies to a specific computer on the network.

Quality of Service

Add QoS Rule

Interface	WAN Outbound		
Application			
Packet Type	Any		
Guaranteed	1	%	
Maximum	100	%	
Priority	0 (Highest)		
DSCP Marking	Disabled		
Address Type	<input type="radio"/> IP Address <input checked="" type="radio"/> MAC Address		
Source MAC Address	11:11:11:11:11:11		
Source Port Range	From	To	
Destination Port Range	From	To	

Apply

2.2.7 DiffServ (DSCP Marking)

DiffServ (a.k.a. DSCP Marking) allows you to classify traffic based on IP DSCP values. These markings can be used to identify traffic within the network. Other interfaces can match traffic based on the DSCP markings. DSCP markings are used to decide how packets should be treated, and is a useful tool to give precedence to varying types of data.

Quality of Service	
Add QoS Rule	
Interface	WAN Outbound
Application	<input type="text"/>
Packet Type	Any
Guaranteed	1 %
Maximum	100 %
Priority	3 (Normal)
DSCP Marking	Disabled
Address Type	<input type="text"/>
Source MAC Address	<input type="text"/>
Source Port Range	To <input type="text"/>
Destination Port Range	To <input type="text"/>
<input type="button" value="Apply"/>	

2.3 Virtual Private Networking

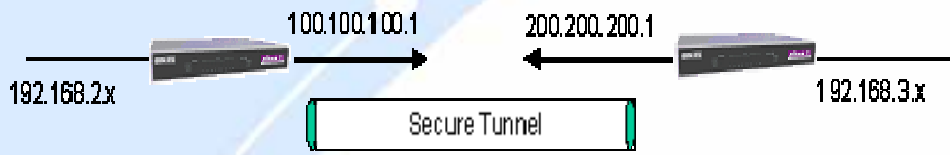
A Virtual Private Network (VPN) enables you to send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link. As such, it is perfect for connecting branch offices to headquarter across the Internet in a secure fashion.

The following section discusses Virtual Private Networking with BiGuard 2/10.

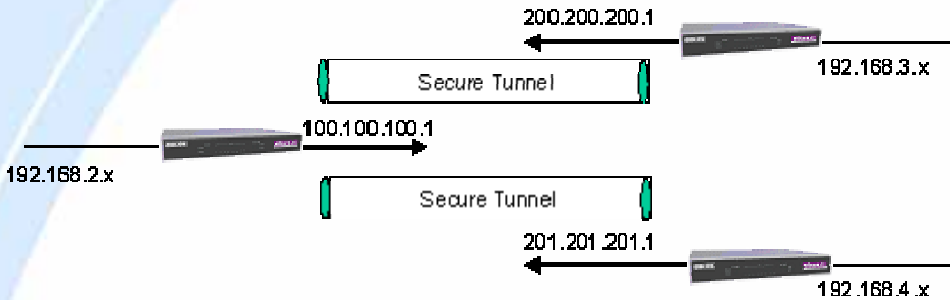
2.3.1 General VPN Setup

There are typically three different VPN scenarios. The first is a **Gateway to Gateway** setup, where two remote gateways communicate over the Internet via a

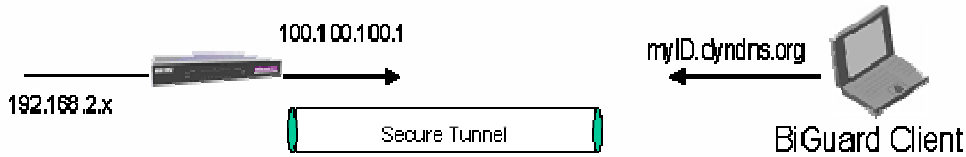
secure tunnel.



The next type of VPN setup is the **Gateway to Multiple Gateway** setup, where one gateway (Headquarter) is communicating with multiple gateways (Branch Offices) over the Internet. As with all VPNs, data is kept secure with secure tunnels.



The final type of VPN setup is the **Client to Gateway**. A good example of where this can be applied is when a remote sales person accesses the corporate network over a secure VPN tunnel.



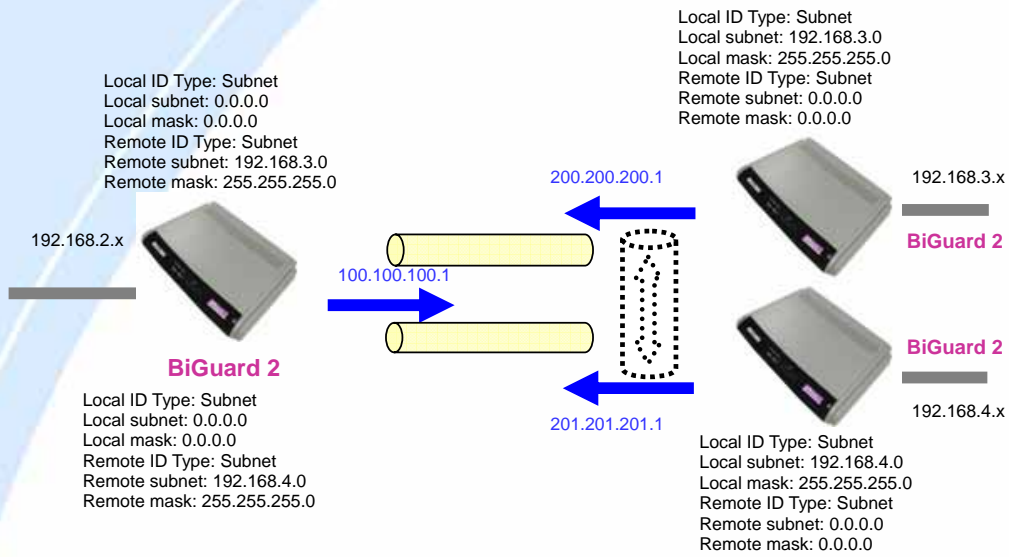
VPN provides a flexible, cost-efficient, and reliable way for companies of all sizes to stay connected. One of the most important steps in setting up a VPN is proper planning. The following sections demonstrate the various ways of using BiGuard 2/10 to setup your VPN.

2.3.2 Concentrator

The VPN Concentrator provides an easy way for branch offices to connect to headquarter through a VPN tunnel. All branch office traffic will be redirected to the VPN tunnel to headquarter with the exception of LAN-side traffic. This way, all branch offices can connect to each other through headquarter via the headquarter's firewall management. You can also configure BiGuard 2/10 to function as a VPN

Concentrator:

Please refer to appendix H for example settings.



Chapter 3: Getting Started

3.1 Overview

BiGuard 2/10 is designed to be a powerful and flexible network device that is also easy to use. With an intuitive web-based configuration, BiGuard 2/10 allows you to administer your network via virtually any Java-enabled web browser and is fully compatible with Linux, Mac OS, and Windows 98/Me/NT/2000/XP operating systems.

The following chapter takes you through the very first steps to configuring your network for BiGuard 2/10. Take a look and see how easy it is to get your network up and running.

3.2 Before You Begin

BiGuard 2/10 is a flexible and powerful networking device. To simplify the configuration process and increase the efficiency of your network, consider the following items before setting up your network for the first time:

1. Plan your network

You may need a fully qualified domain name either for convenience or if you have a dynamic IP address. See Chapter 2: Router Applications for more information.

2. Set up your accounts

Have access to the Internet and locate the Internet Service Provider (ISP) configuration information.

3. Determine your network management approach

BiGuard 2/10 is capable of remote management. However, this feature is not active by default. If you reset the device, remote administration must be enabled again. If you decide to manage your network remotely, be sure to change the default password to something more secure.

4. Prepare to physically connect BiGuard 2/10 to Cable or DSL modems and a computer.

Be sure to also review the Safety Warnings located in the preface of this manual before working with your BiGuard 2/10.

3.3 Connecting Your Router

Connecting BiGuard 2/10 is an easy three-step process:

1. Connect BiGuard 2/10 to your LAN by connecting Ethernet cables from your networked PCs to the LAN ports on the router. Connect BiGuard 2/10 to your broadband Internet connection via router's WAN port.



2. Plug BiGuard 2/10 to an AC outlet with the included AC Power Adapter.



3. Ensure that the Power and WAN LEDs are solidly lit, and that on any LAN port that has an Ethernet cable plugged in the LED is also solidly lit. The Status LED will remain solid as the device boots. Once the boot sequence is complete, the LED will shut off, indicating that BiGuard 2/10 is ready.



If the router does not power on, please refer to **Chapter 5: Troubleshooting** for possible solutions.

3.4 Configuring PCs for TCP/IP Networking

Now that your BiGuard 2/10 is connected properly to your network, it's time to configure your networked PCs for TCP/IP networking.

In order for your networked PCs to communicate with your router, they must have the following characteristics:

1. Have a properly installed and functioning Ethernet Network Interface Card (NIC).
2. Be connected to BiGuard 2/10, either directly or through an external repeater hub via an Ethernet cable.
3. Have TCP/IP installed and configured with an IP address.

The IP address for each PC may be a fixed IP address or one that is obtained from a DHCP server. If using a fixed IP address, it is important to remember that it must be in the same subnet as the router. The default IP address of BiGuard 2/10 is 192.168.1.254 with a subnet mask of 255.255.255.0. Using the default configuration, networked PCs must reside in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253. However, you'll find that the quickest and easiest way to configure the IP addresses for your PCs is to obtain the IP addresses automatically by using the router as a DHCP server.

If you are unable to access the web configuration interface, check to see if you have any software-based firewalls installed on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of BiGuard 2/10.

The following sections outline how to set up your PCs for TCP/IP networking. Refer to the applicable section for your PC's operating system.

3.4.1 Overview

Before you begin, make sure that the TCP/IP protocol and a functioning Ethernet network adapter is installed on each of your PCs.

The following operating systems already include the necessary software components you need to install TCP/IP on your PCs:

- Windows 95/98/Me/NT/2000/XP

- Mac OS 7 and later
- All versions of UNIX/Linux

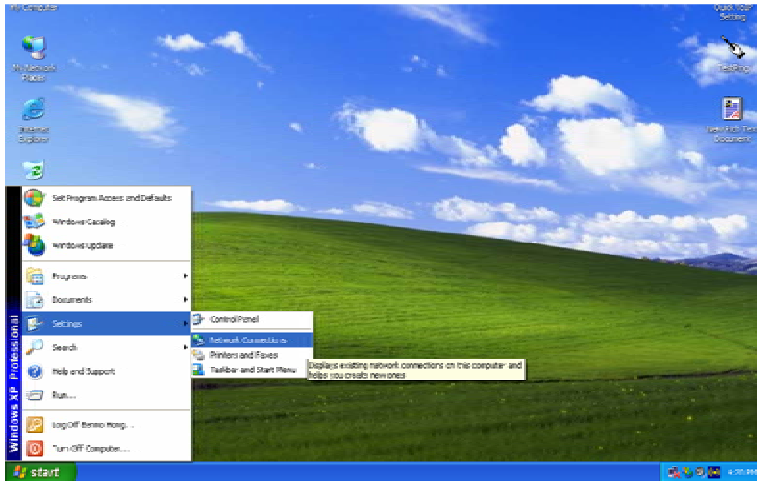
If you are using Windows 3.1, you must purchase a third-party TCP/IP application package.

Any TCP/IP capable workstation can be used to communicate with or through the BiGuard 2/10. To configure other types of workstations, please consult the manufacturer's documentation.

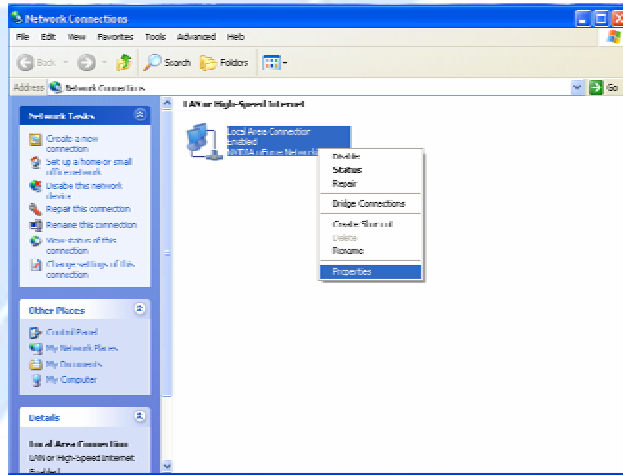
3.4.2 Windows XP

3.4.2.1 Configuring

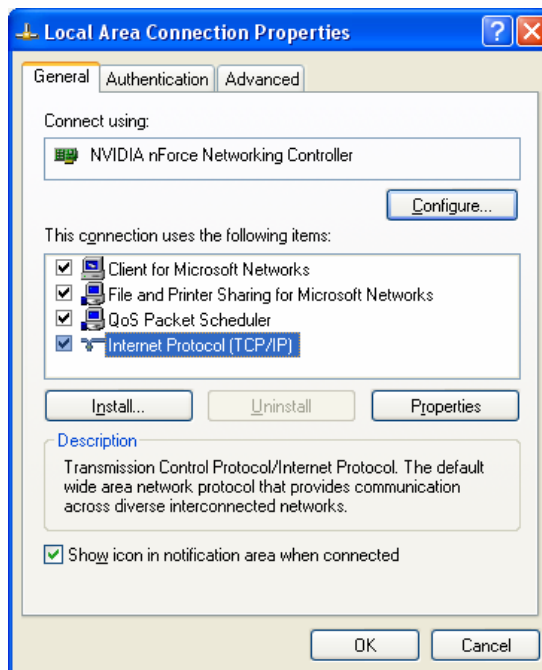
1. Select **Start > Settings > Network Connections**.



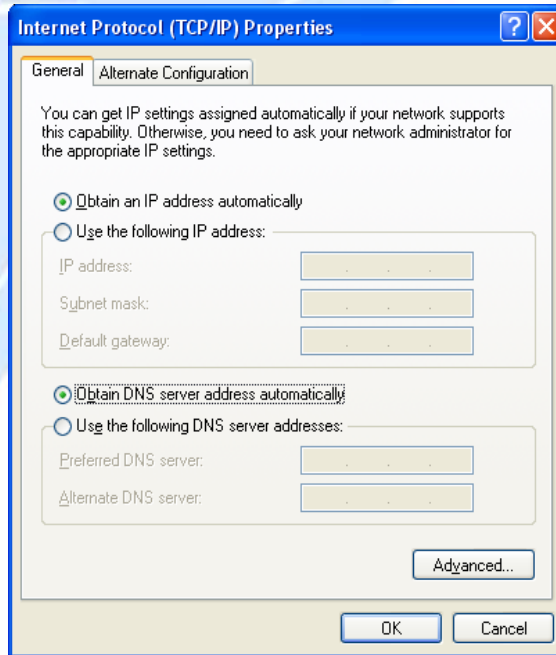
2. In the **Network Connections** window, right-click **Local Area Connection** and select **Properties**.



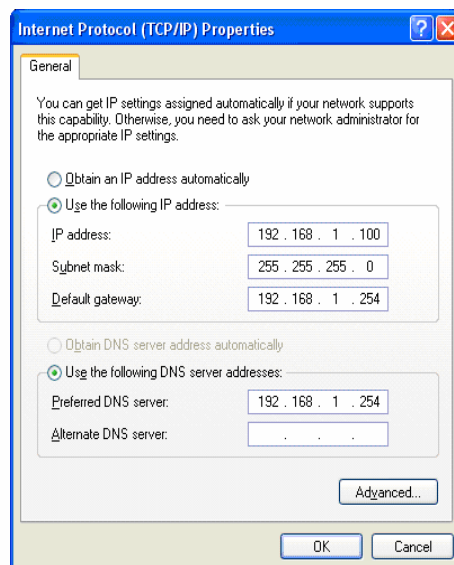
3. Select **Internet Protocol (TCP/IP)** and click **Properties**.



4a. To have your PC obtain an IP address automatically, select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons.



4b. To manually assign your PC a fixed IP address, select the **Use the following IP address** radio button and enter your desired IP address, subnet mask, and default gateway in the blanks provided. Remember that your PC must reside in the same subnet mask as the router. To designate a DNS server, select the **Use the following DNS server** and fill in the preferred DNS address.



5. Click **OK** to finish the configuration.

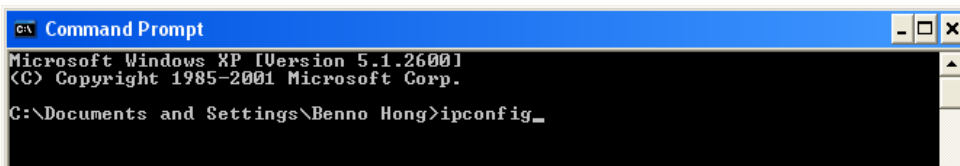
3.4.2.2 Verifying Settings

To verify your settings using a command prompt:

1. Click **Start > Programs > Accessories > Command Prompt.**

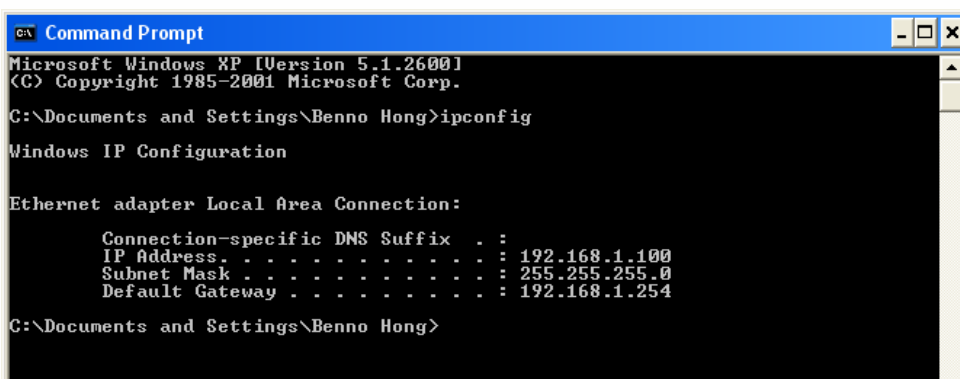


2. In the Command Prompt window, type `ipconfig` and then press **ENTER**.



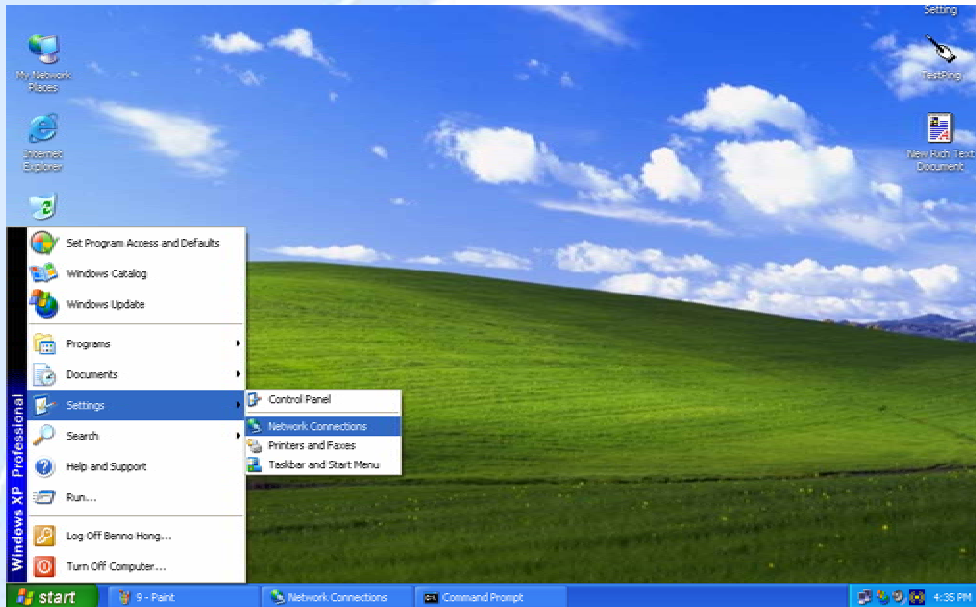
If you are using BiGuard 2/10's default settings, your PC should have:

- An IP address between 192.168.1.1 and 192.168.1.253
- A subnet mask of 255.255.255.0

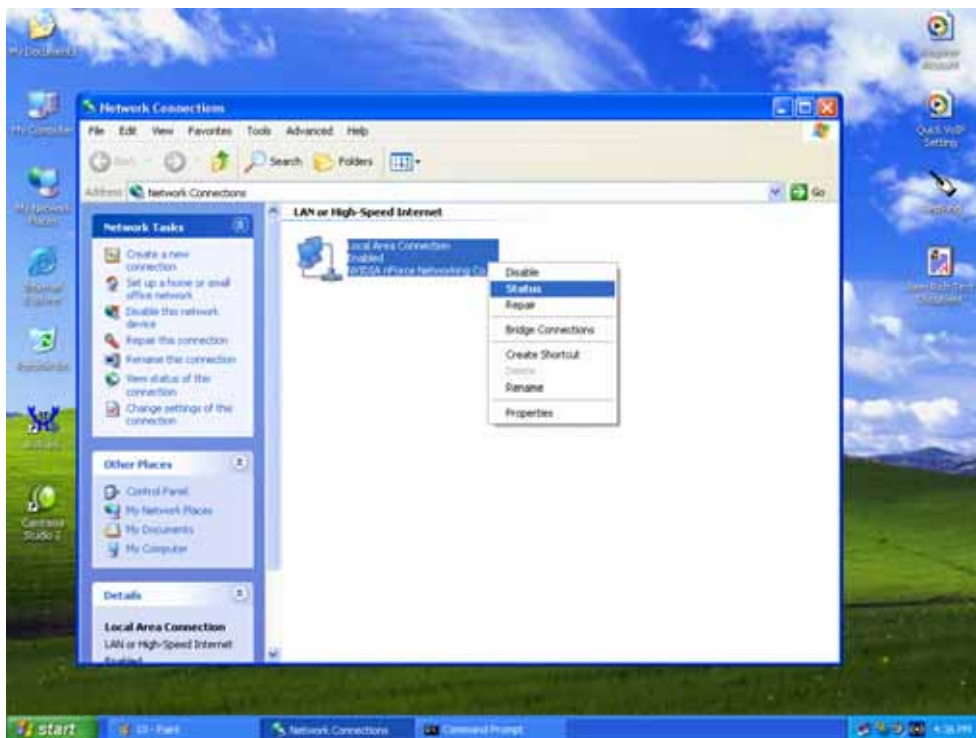


To verify your settings using the Windows XP GUI:

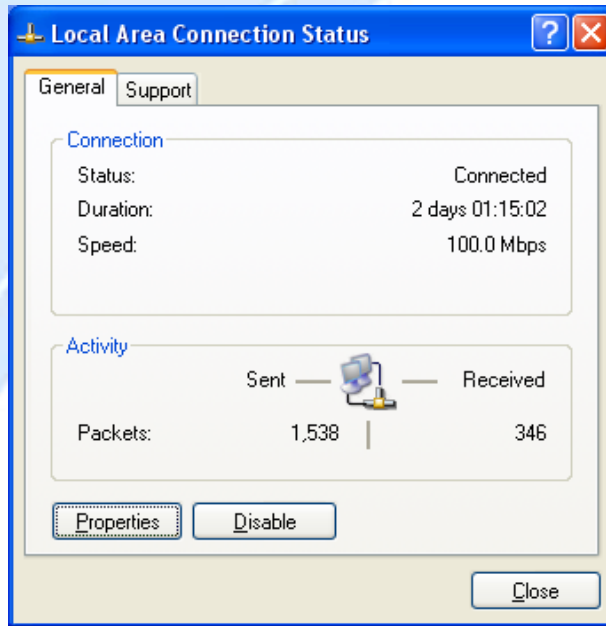
1. Click **Start** > **Settings** > **Network Connections**.



2. Right click one of the network connections listed and select **Status** from the pop-up menu.

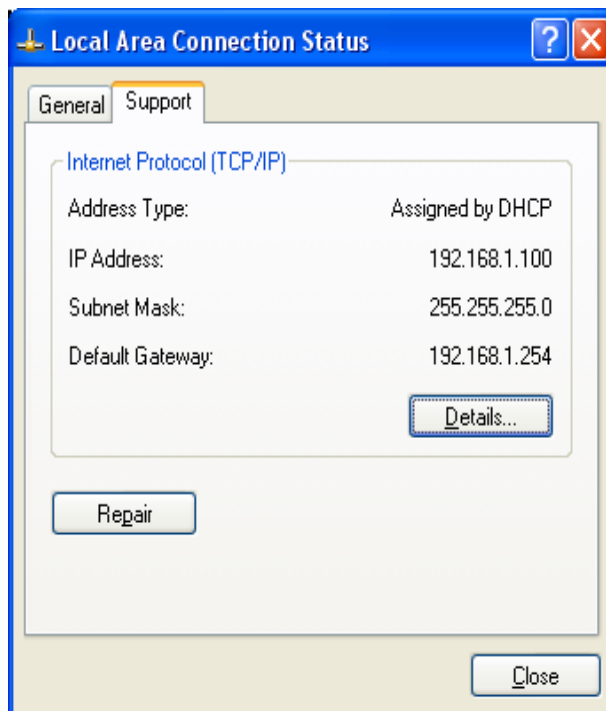


3. Click the **Support** tab.



If you are using BiGuard 2/10's default settings, your PC should:

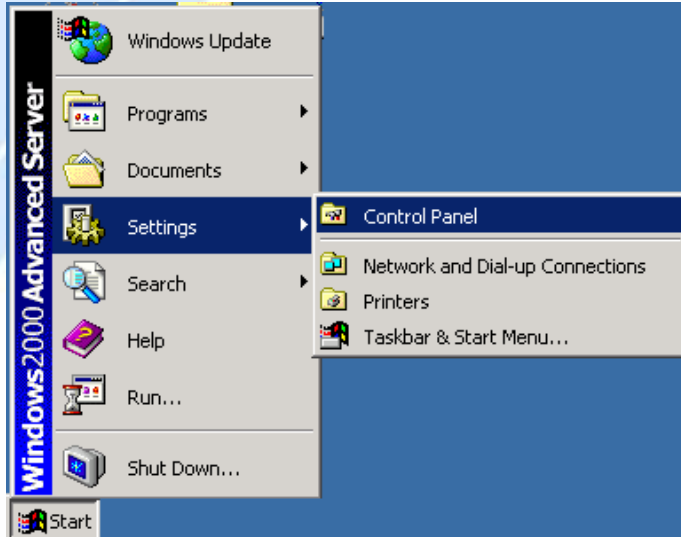
- Have an IP address between 192.168.1.1 and 192.168.1.253
- Have a subnet mask of 255.255.255.0



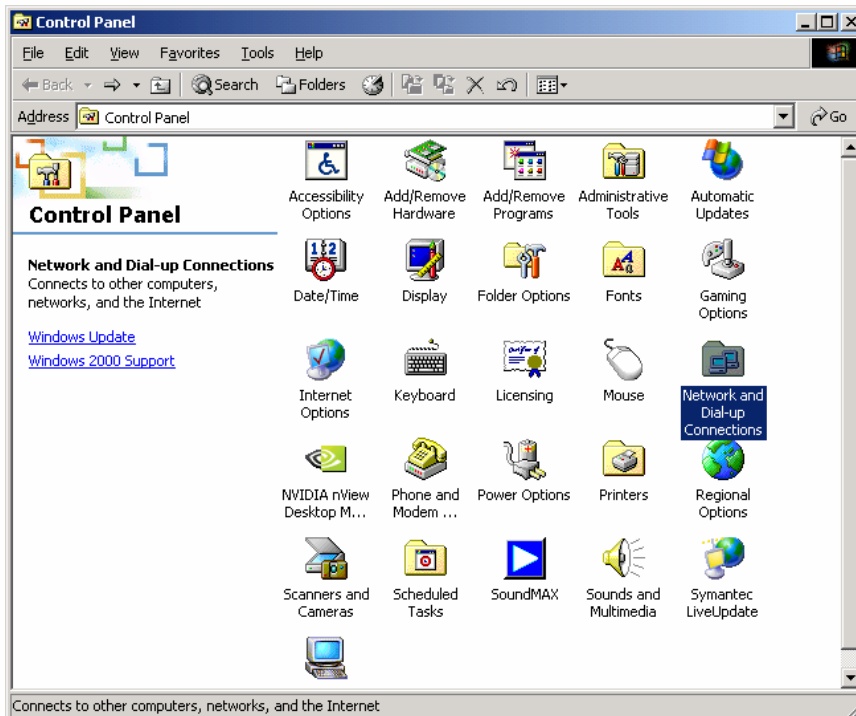
3.4.3 Windows 2000

3.4.3.1 Configuring

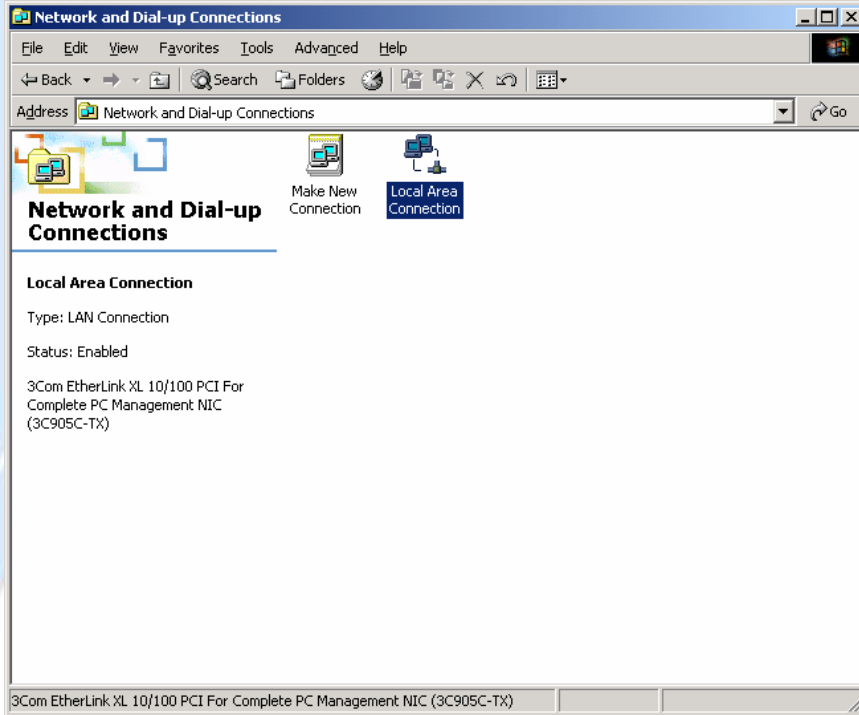
1. Select **Start > Settings > Control Panel**.



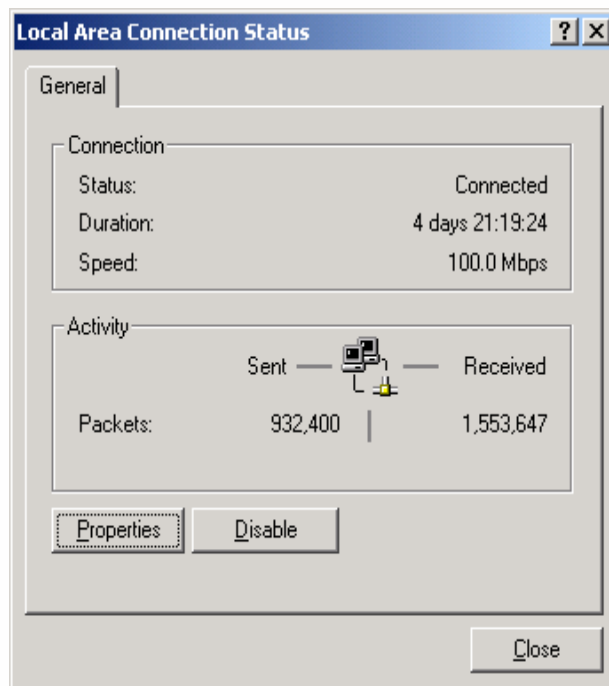
2. In the Control Panel window, double-click **Network and Dial-up Connections**.



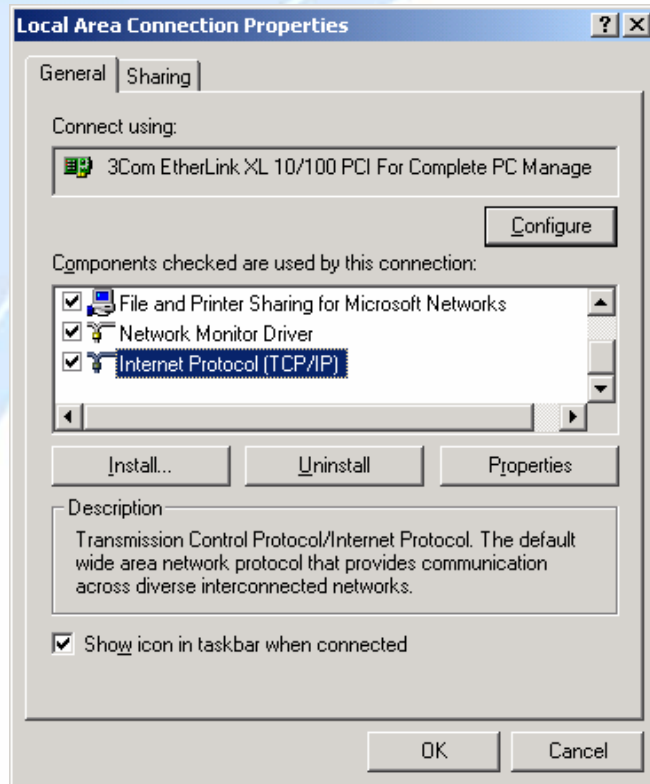
3. In Network and Dial-up Connections, double-click **Local Area Connection**.



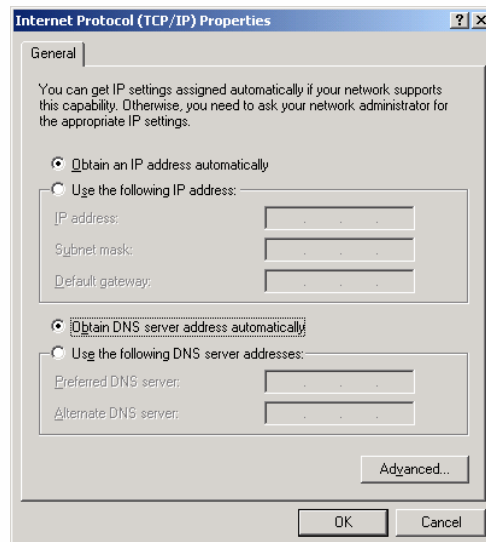
4. In the Local Area Connection window, click **Properties**.



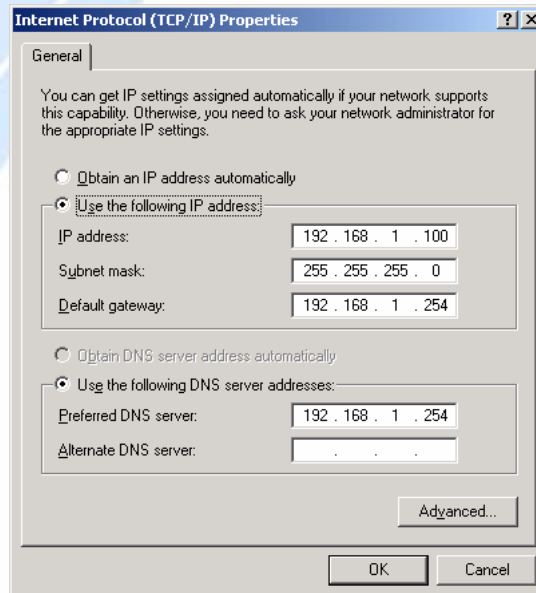
5. Select **Internet Protocol (TCP/IP)** and click **Properties**.



6a. To have your PC obtain an IP address automatically, select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons.



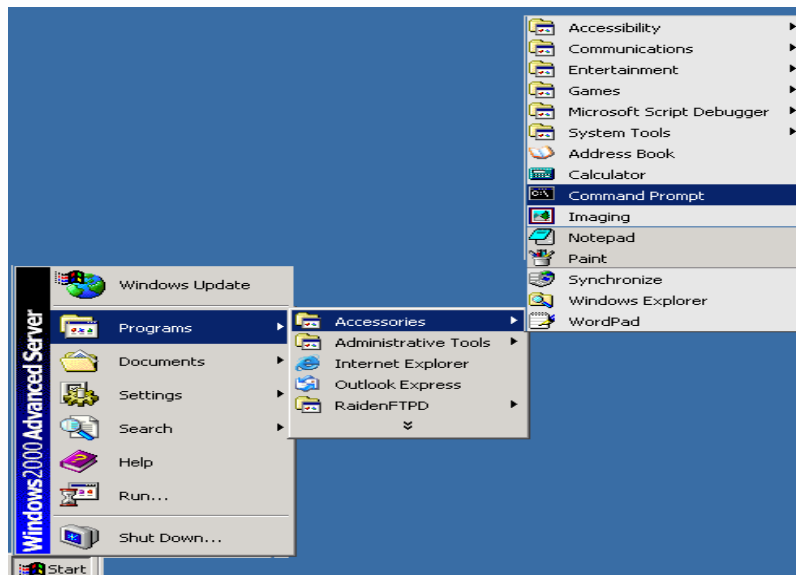
6b. To manually assign your PC a fixed IP address, select the **Use the following IP address** radio button and enter your desired IP address, subnet mask, and default gateway in the blanks provided. Remember that your PC must reside in the same subnet mask as the router. To designate a DNS server, select the **Use the following DNS server** and fill in the preferred DNS address.



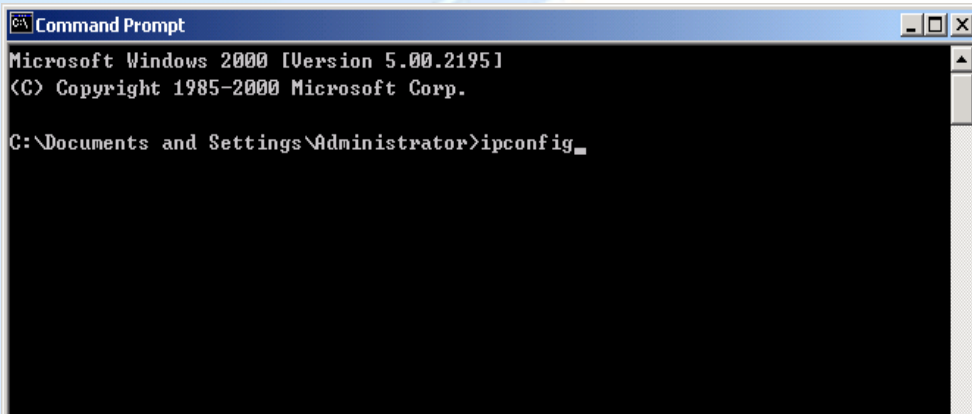
7. Click **OK** to finish the configuration.

3.4.3.2 Verifying Settings

1. Click **Start > Programs > Accessories > Command Prompt**.

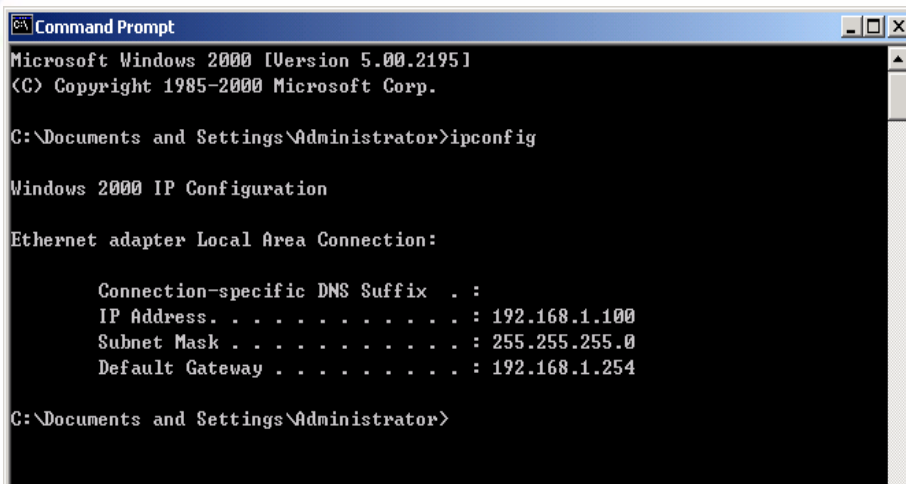


2. In the Command Prompt window, type `ipconfig` and then press **ENTER**.



If you are using BiGuard 2/10's default settings, your PC should have:

- An IP address between 192.168.1.1 and 192.168.1.253
- A subnet mask of 255.255.255.0

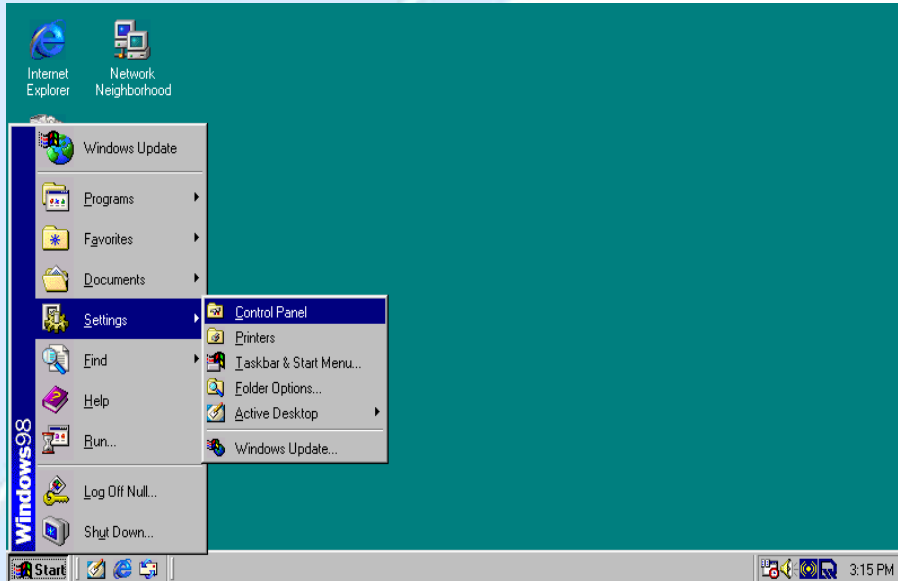


3.4.4 Windows 98 / Me

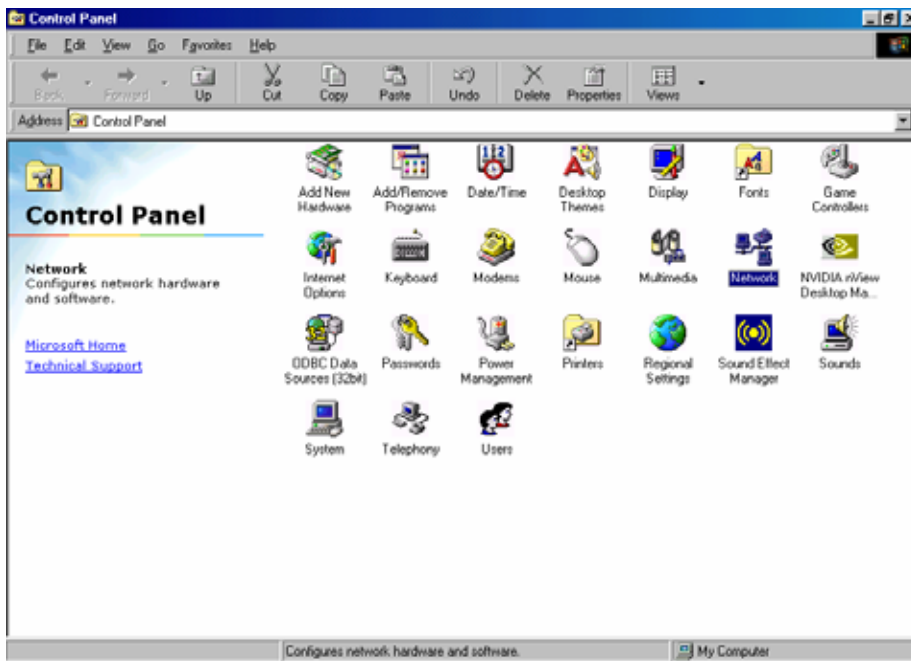
3.4.4.1 Installing Components

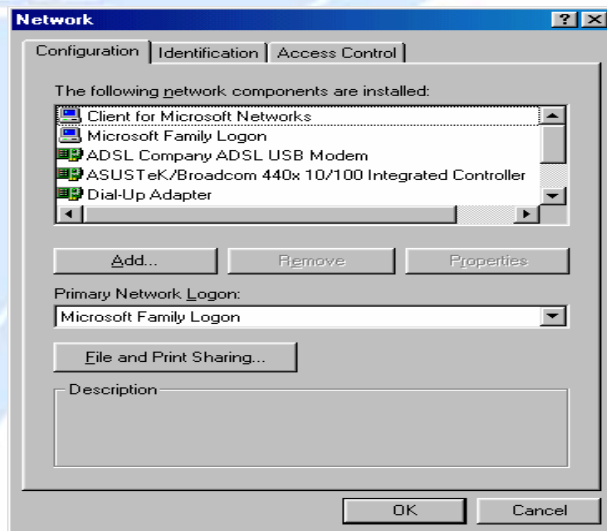
To prepare Windows 98/Me PCs for TCP/IP networking, you may need to manually install TCP/IP on each PC. To do this, follow the steps below. Be sure to have your Windows CD handy, as you may need to insert it during the installation process.

1. On the Windows taskbar, select **Start** > **Settings** > **Control Panel**.



2. Double-click the **Network** icon. The Network window displays a list of installed components.



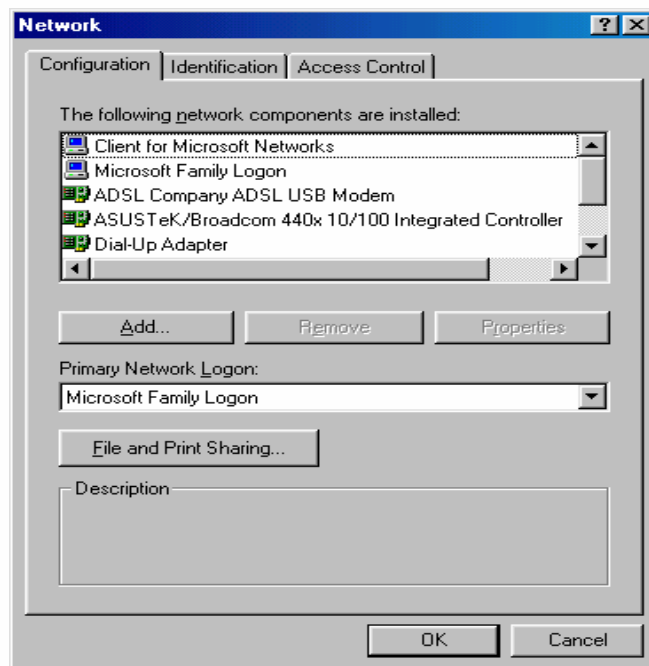


You must have the following installed:

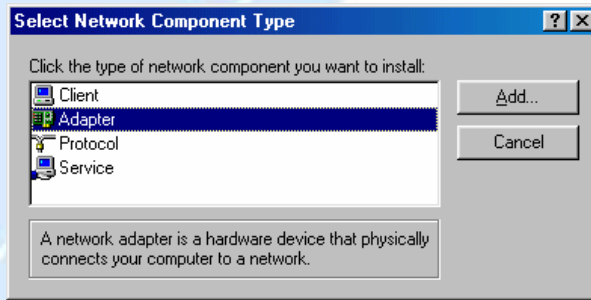
- An Ethernet adapter
- TCP/IP protocol
- Client for Microsoft Networks

If you need to install a new Ethernet adapter, follow these steps:

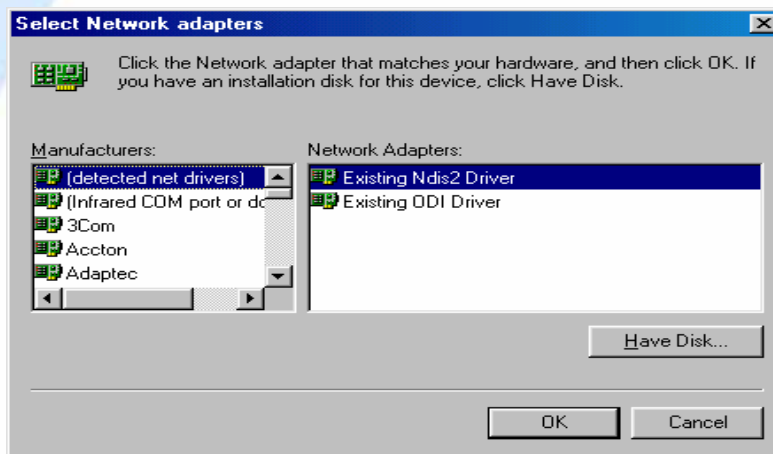
- a. Click **Add**.



b. Select **Adapter**, then **Add**.

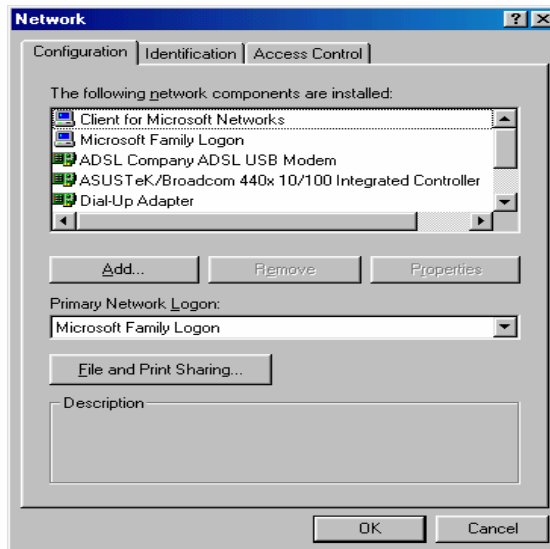


c. Select the manufacturer and model of your Ethernet adapter, then click **OK**.

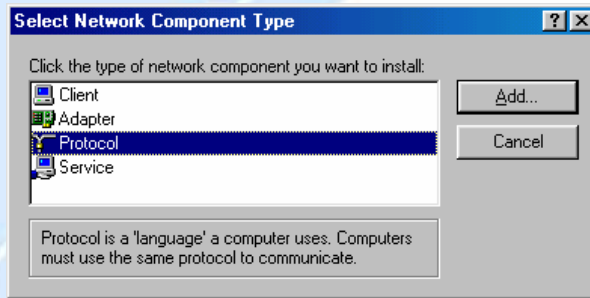


If you need TCP/IP:

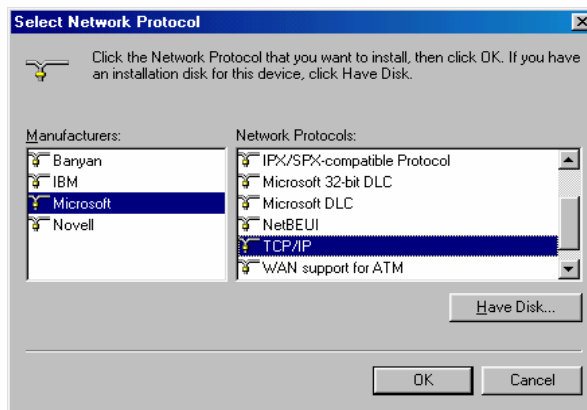
a. Click **Add**.



b. Select **Protocol**, then click **Add**.

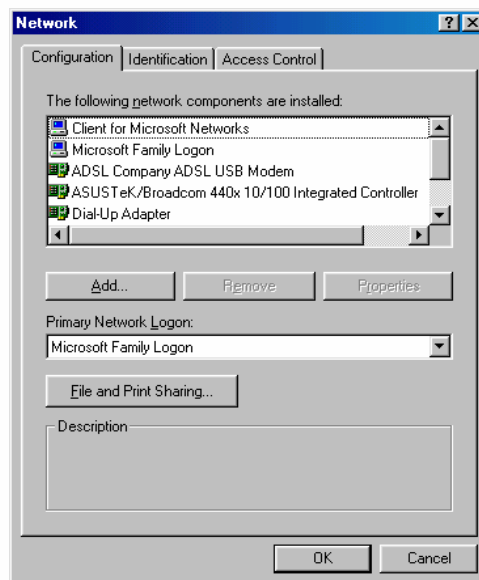


c. Select **Microsoft**. → **TCP/IP**, then **OK**.

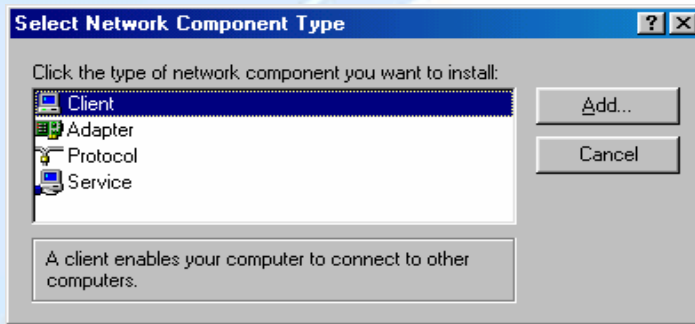


If you need Client for Microsoft Networks:

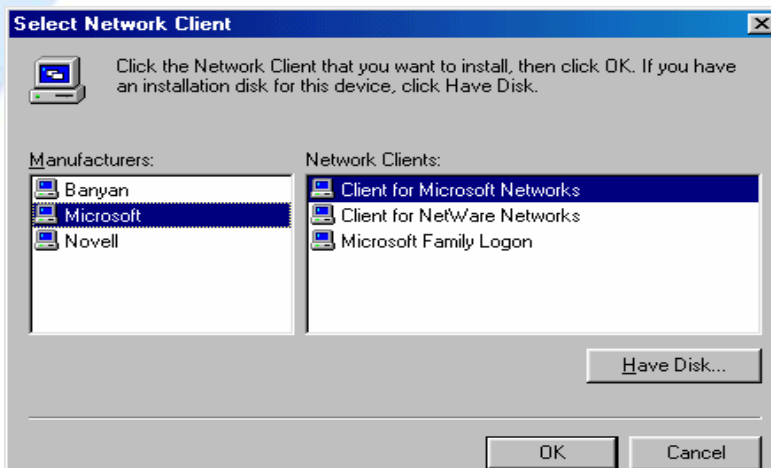
a. Click **Add**.



b. Select **Client**, then click **Add**.



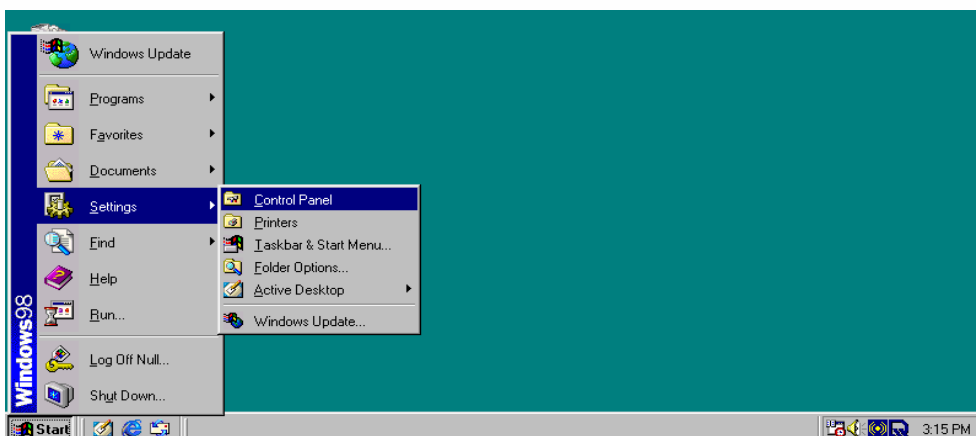
c. Select **Microsoft**. → **Client for Microsoft Networks**, and then click **OK**.



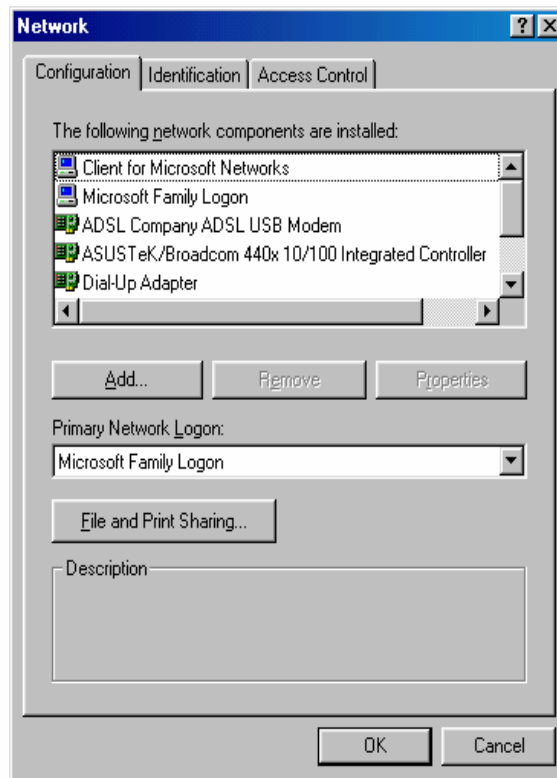
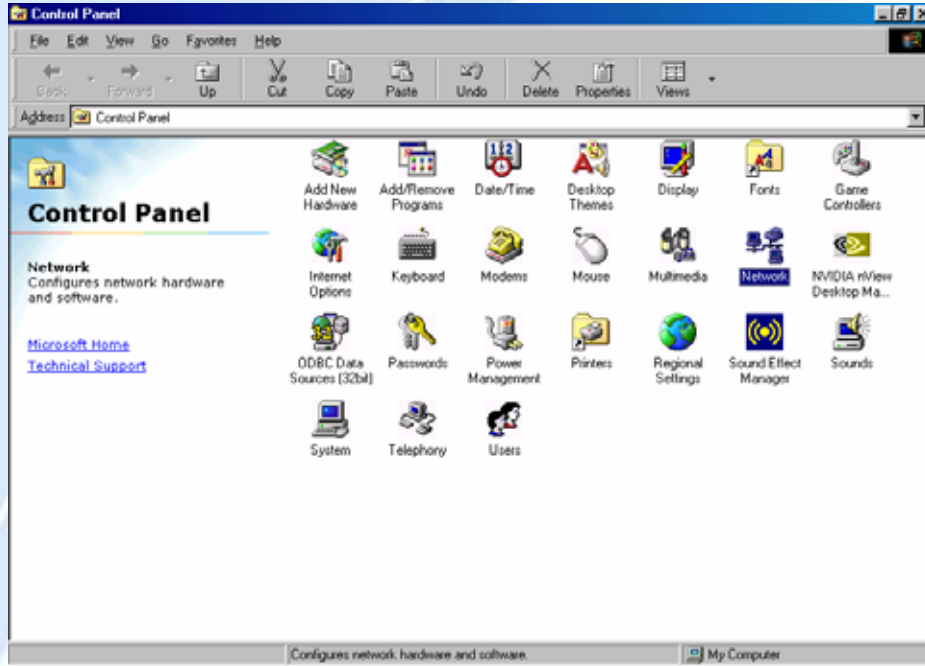
3. Restart your PC to apply your changes.

3.4.4.2 Configuring

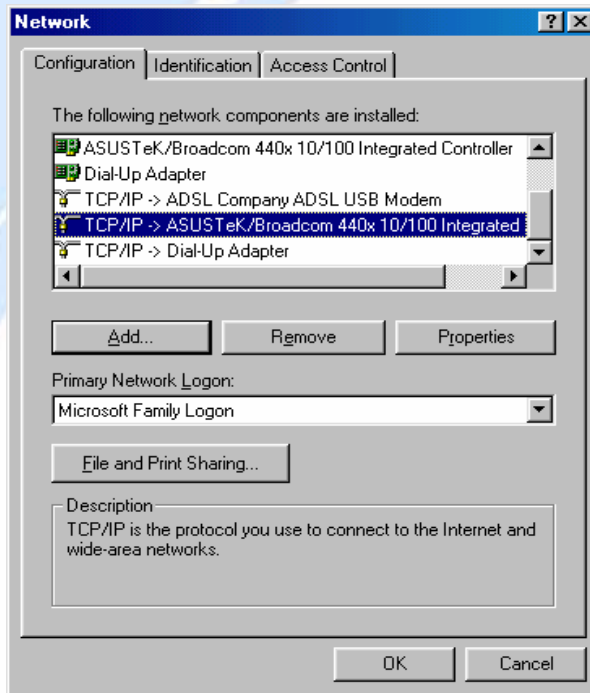
1. Select **Start > Settings > Control Panel**.



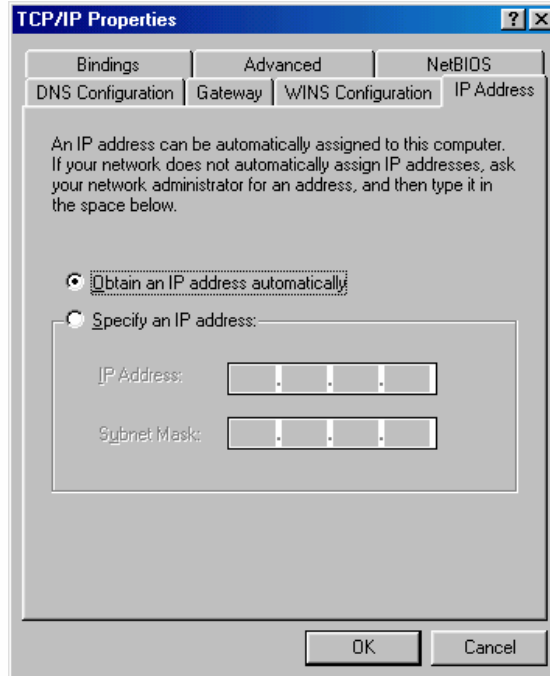
2. In the Control Panel, double-click **Network** and choose the **Configuration** tab.



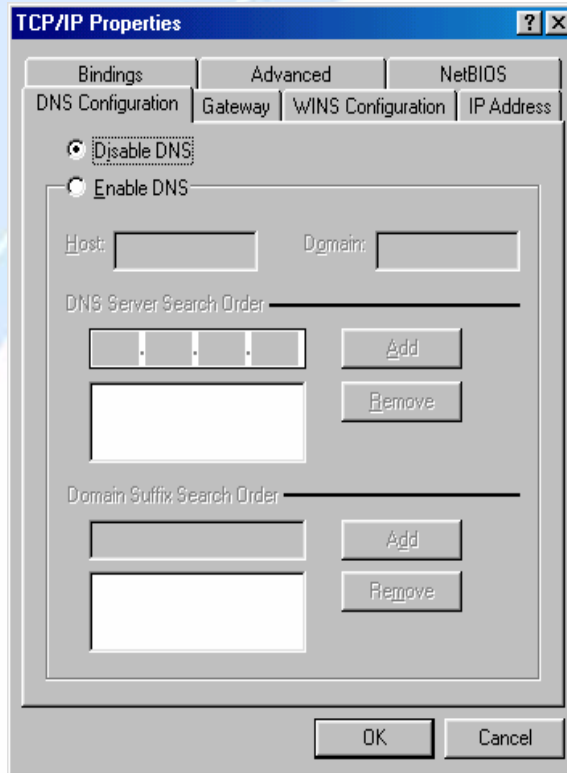
3. Select the name of your PC's **TCP/IP** Network Interface Card (NIC) and click **Properties**. TCP/IP > ASUSTeK is illustrated in the example below.



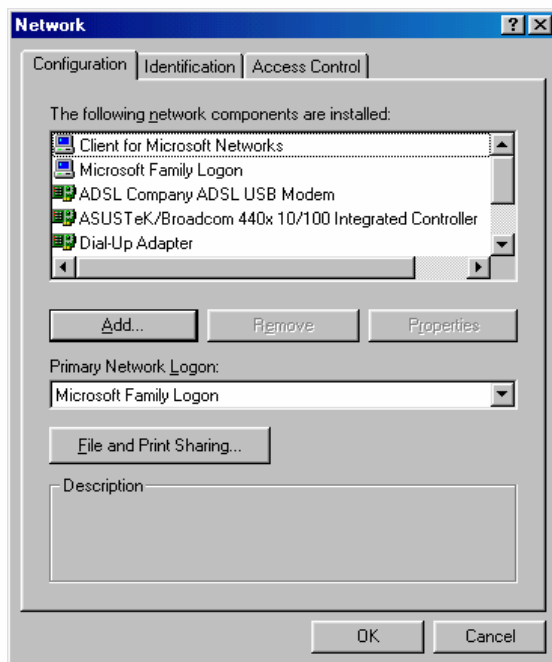
4. Select the **IP Address** tab and click the **Obtain an IP address automatically** radio button.



5. Select the **DNS Configuration** tab and select the **Disable DNS** radio button.



6. Click **OK** to apply the configuration.



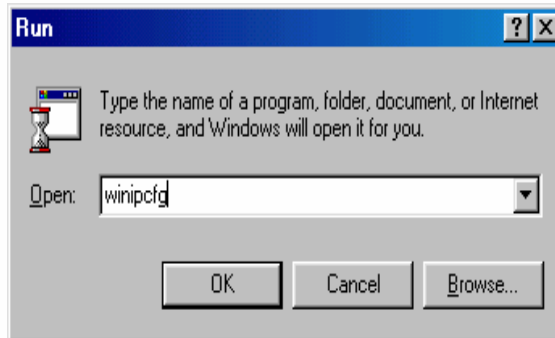
3.4.4.3 Verifying Settings

To check the TCP/IP configuration, use the winipcfg.exe utility:

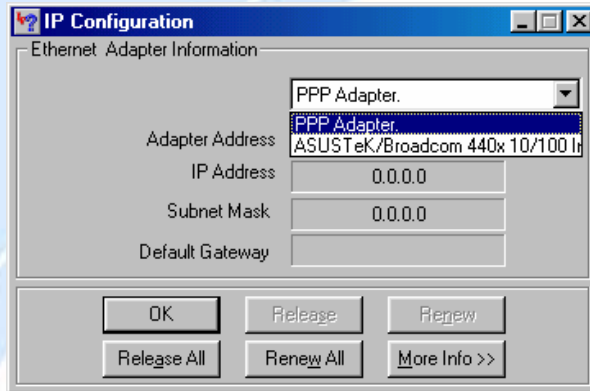
1. Select **Start > Run**.



2. Type winipcfg, and then click **OK**.

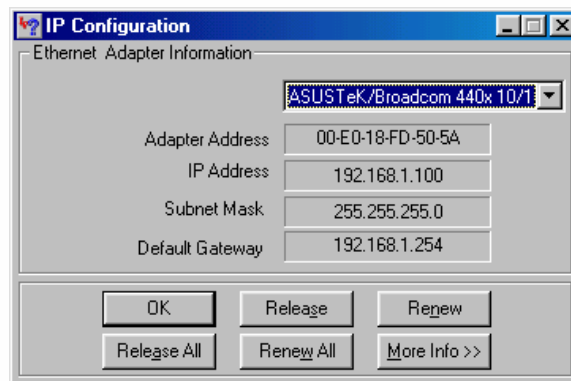


3. From the drop-down box, select your Ethernet adapter.



The window is updated to show your settings. Using the default BiGuard 2/10 settings, your PC should have:

- An IP address between 192.168.1.1 and 192.168.1.253
- A subnet mask of 255.255.255.0
- A default gateway of 192.168.1.254



3.5 Factory Default Settings

Before configuring your BiGuard 2/10, you need to know the following default settings:

Web Interface:

Username: admin

Password: admin

LAN Device IP Settings:

IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

ISP setting in WAN site:
Obtain an IP Address automatically (DHCP Client)

DHCP server:
DHCP server is enabled.
Start IP Address: 192.168.1.100
End IP Address: 192.168.1.199

3.5.1 Username and Password

The default user name and password are "admin" and "admin" respectively. If you ever forget your user name and/or password, you can restore your BiGuard 2/10 to its factory settings by holding the Reset button on the back of your router until the Status LED begins to blink. Please note that doing this will also erase any previous router settings that you have made. The Status LED will remain solid as the device boots. Once the boot sequence is complete, the LED will shut off, indicating that BiGuard 2/10 is ready.

3.5.2 LAN and WAN Port Addresses

The default values for LAN and WAN ports are shown below:

LAN Port		WAN Port
IP address	192.168.1.254	The DHCP Client is <i>enabled</i> to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

3.6 Information From Your ISP

3.6.1 Protocols

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP, Static IP, PPPoE, or PPTP. The following table outlines each of these protocols:

DHCP	Configure this WAN interface to use DHCP client protocol to get an IP address from your ISP automatically. Your ISP provides an IP address to the router dynamically when logging in.
Static IP	Configure this WAN interface with a specific IP address. This IP address should be provided by your ISP.
PPPoE	PPPoE (PPP over Ethernet) is known as a dial-up DSL or cable service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure.
PPTP	If your ISP provides a PPTP connection, you can use the PPTP protocol to establish a connection to your ISP.
Big Pond	The Big Pond login for Telstra cable in Australia.

If your account uses PPP over Ethernet (PPPoE), you will need to enter your login name and password when configuring your BiGuard 2/10. After the network and firewall are configured, BiGuard 2/10 will login automatically, and you will no longer need to run the login program from your PC.

3.6.2 Configuration Information

If your ISP does not dynamically assign configuration information but instead uses fixed configurations, you will need the following basic information from your ISP:

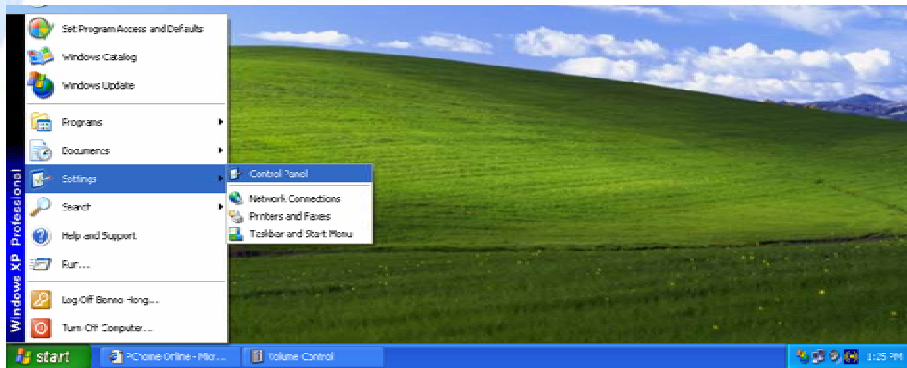
- An IP address and subnet mask
- A gateway IP address
- One or more domain name server (DNS) IP addresses

Depending on your ISP, a host name and domain suffix may also be provided. If any of these items are dynamically supplied by the ISP, your BiGuard 2/10 will automatically acquire them.

If an ISP technician configured your computer or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window before reconfiguring your computer for use with BiGuard 2/10. The following sections describe how you can obtain this information.

This section uses illustrations from Windows XP. However, other versions of Windows will follow a similar procedure. Have your Windows CD handy, as it may be required during the configuration process.

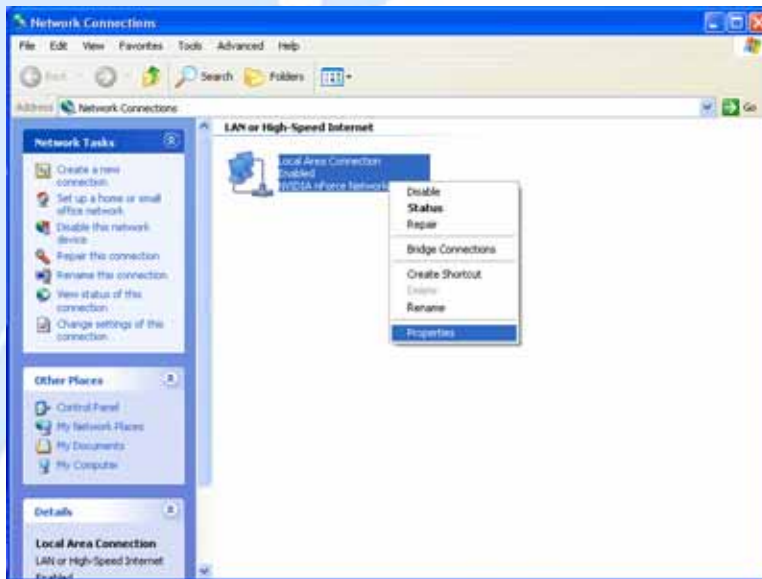
1. Select **Start > Settings > Control Panel**.



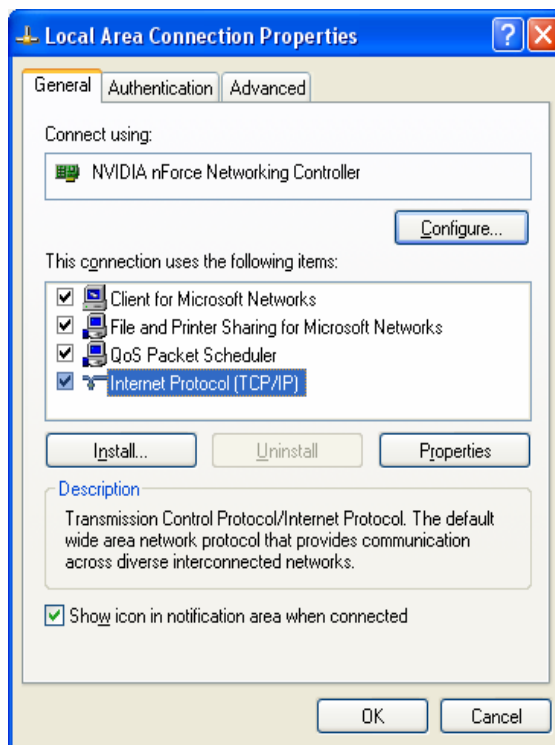
2. Double-click the **Network** icon.



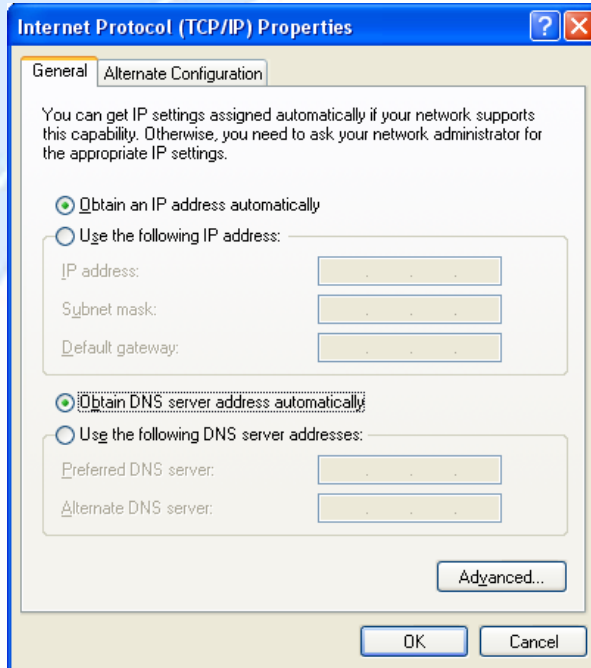
3. In the **Network Connections** window, right-click **Local Area Connection** and select **Properties**.



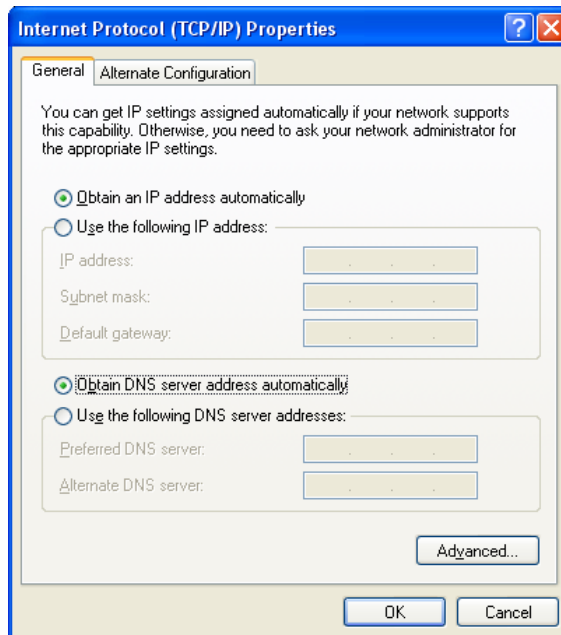
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



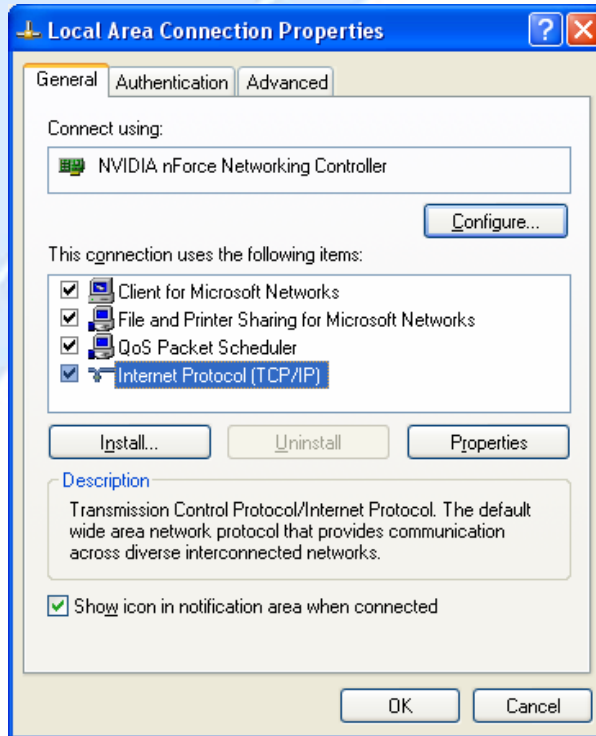
5. If an **IP address**, **subnet mask** and a **Default gateway** are shown, write down the information. If no address is present, your account's IP address is dynamically assigned. **Click the Obtain an IP address automatically** radio button.



6. If any DNS server addresses are shown, write them down. Click the Obtain DNS server address automatically radio button.



7. Click **OK** to save your changes.



3.7 Web Configuration Interface

BiGuard 2/10 includes a Web Configuration Interface for easy administration via virtually any browser on your network. To access this interface, open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click **Go**. A user name and password window prompt will appear. Enter your user name and password (the default user name and password are "admin" and "admin") to access the Web Configuration Interface.



The screenshot displays the 'Status' page of the Billion BiGuard 2/10 web configuration interface. The page is divided into several sections: a left-hand navigation menu, a main content area, and a footer with action buttons.

Navigation Menu:

- Status (selected)
- Quick Start
- Configuration
- Save Config to Flash

Main Content Area:

Status Refresh

Device Information

Device Name	BiGuard10
System Up Time	0: 0: 3:20 (day:hour:min:sec)
Current Time	Mon Aug 1 05:03:08 2005 Sync Now
Private LAN MAC Address	00:11:73:24:45:11
Public WAN MAC Address	00:11:73:24:45:00
Firmware Version	1.05
Home URL	Billion Electric Co.,Ltd.

LAN

IP Address	192.168.1.254
Netmask	255.255.255.0
DHCP Server	Enabled

WAN

Connection Method	Connect by DHCP
IP Address	connecting Release Renew
Netmask	
Gateway	
DNS	
Up Time	

Footer: SAVE CONFIG RESTART LOGOUT

If the Web Configuration Interface appears, congratulations! You are now ready to configure your BiGuard 2/10. If you are having trouble accessing the interface, please refer to **Chapter 5: Troubleshooting** for possible resolutions.

Chapter 4: Router Configuration

4.1 Overview

The Web Configuration Interface makes it easy for you to manage your network via any PC connected to it. On the Web Configuration homepage, you will see the navigation pane located on the left hand side. From it, you will be able to select various options used to configure your router.



1. Click **Apply** if you would like to apply the settings on the current screen to the device. The settings will be effective immediately, however the configuration is not saved yet and the settings will be erased if you power off or restart the device.
2. Click **SAVE CONFIG** to save the current settings permanently to the device.
3. Click **RESTART** to restart the device. There are two options to restart the device.
 - Select **Current Settings** if you would like to restart using the current configuration.
 - Select **Factory Default Settings** if you would like to restart using the factory default configuration.
4. To exit the router's web interface, click **LOGOUT**. Please ensure that you have saved your configuration settings before you logout. Be aware that the router is

restricted to only one PC accessing the web configuration interface at a time. Once a PC has logged into the web interface, other PCs cannot gain access until the current PC has logged out. If the previous PC forgets to logout, the second PC can access the page after a user-defined period (5 minutes by default).

The following sections will show you how to configure your router using the Web Configuration Interface.

4.2 Status

The Status menu displays the various options that have been selected and a number of statistics about your BiGuard 2/10. In this menu, you will find the following sections:

- ARP Table
- Routing Table
- Session Table
- DHCP Table
- IPSec Status
- PPTP Status
- System Log
- IPSec Log



Status
ARP Table
Routing Table
Session Table
DHCP Table
IPSec Status
PPTP Status
System Log
IPSec Log

4.2.1 ARP Table

The Address Resolution Protocol (ARP) Table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way to determine the MAC

address of your PC's network interface to use with the router's Firewall – MAC Address Filter function. See the **Firewall** section of this chapter for more information on this feature.

Status	ARP Table				
ARP Table	IP <-> MAC List				
Routing Table	No.	IP Address	MAC Address	Interface	Static
Session Table	1	192.168.1.100	00:50:BA:F0:18:26	LAN	no
DHCP Table					
IPSec Status					
PPTP Status					
System Log					
IPSec Log					
Quick Start					
Configuration					
Save Config to Flash					

No.: Number of the list.

IP Address: A list of IP addresses of devices on your LAN.

MAC Address: The Media Access Control (MAC) addresses for each device on your LAN.

Interface: The interface name (on the router) that this IP address connects to.

Static: Static status of the ARP table entry.

NO indicates dynamically-generated ARP table entries.

YES indicates static ARP table entries added by the user.

4.2.2 Routing Table

The Routing Table displays the current path for transmitted packets. Both static and dynamic routes are displayed.

Status	Routing Table				
ARP Table	Routing Table				
Routing Table	No.	Destination	Netmask	Gateway/Interface	Cost
Session Table	1	192.168.1.0	255.255.255.0	0.0.0.0/ LAN	0
DHCP Table					
IPSec Status					
PPTP Status					
System Log					
IPSec Log					
Quick Start					
Configuration					
Save Config to Flash					

No.: Number of the list.

Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway/Interface: The IP address of the gateway or existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

4.2.3 Session Table

The NAT Session Table displays a list of current sessions for both incoming and outgoing traffic with protocol type, source IP, source port, destination IP and destination port, each page shows 10 sessions.

No.	Protocol	From IP	From Port	To IP	To Port
1	TCP	192.168.1.100	2922	192.168.1.254	80
2	TCP	192.168.1.100	2923	192.168.1.254	80
3	TCP	192.168.1.100	2924	192.168.1.254	80
4	TCP	192.168.1.100	2925	192.168.1.254	80
5	TCP	192.168.1.100	2926	192.168.1.254	80
6	TCP	192.168.1.100	2928	192.168.1.254	80

Session 1 - 6 of 6, 1/1.

Filter: From IP: [] From Port: [] To IP: [] To Port: []

First Previous Next Last Jump to session GO

No.: Number of the list.

Protocol: Protocol type of the Session.

From IP: Source IP of the session.

From port: source port of the session.

To IP: Destination IP of the session.

To port: Destination port of the session.

Sessions:

Filter: when the presented field is filled, please click Filter button.

From IP: please input the source IP you would like to filter.

From port: please input the source port you would like to filter.

To IP: please input the destination IP you would like to filter.

To port: please input the destination port you would like to filter.

First: To the first page.

Previous: To the previous page.

Next: To the next page.

Last: To the last page.

Jump to the session: please input the session number you would like to see and press "GO"

4.2.4 DHCP Table

The DHCP Table displays a list of IP addresses that have been assigned to PCs on your network via Dynamic Host Configuration Protocol (DHCP).

No.	IP Address	Device Name	MAC Address	Lease Time
1	192.168.1.100	TEST-DNS	00:50:ba:d0:16:26	254009

No.: Number of the list.

IP Address: A list of IP addresses of devices on your LAN.

Device Name: The host name (computer name) of the client.

MAC Address: The MAC address of client.

4.2.5 IPsec Status

The IPsec Status window displays the status of the IPsec Tunnels that are currently configured on your BiGuard 2/10.

Name	Enable	Status	Local Network	Remote Network	Remote Gateway	SA	Action
------	--------	--------	---------------	----------------	----------------	----	--------

Name: The name you assigned to the particular IPsec entry.

Enable: Whether the IPSec connection is currently Enable or Disable.

Status: Whether the IPSec is Active, Inactive or Disable.

Local Subnet: The local IP address or subnet used.

Remote Subnet: The subnet of the remote site.

Remote Gateway: The remote gateway IP address.

SA: The Security Association for this IPSec entry.

Action: Manually connect or drop the tunnel.

4.2.6 PPTP Status

The PPTP Status window displays the status of the PPTP Tunnels that are currently configured on your BiGuard 2/10.

PPTP Status						
PPTP Accounts						
Name	Enable	Status	Type	Peer Network	Connect By	Action

Name: The name you assigned to the particular PPTP entry.

Enable: Whether the PPTP connection is currently Enable or Disable.

Status: Whether the PPTP is Active, Inactive or Disable.

Type: Whether the Connection type is Remote Access or LAN to LAN

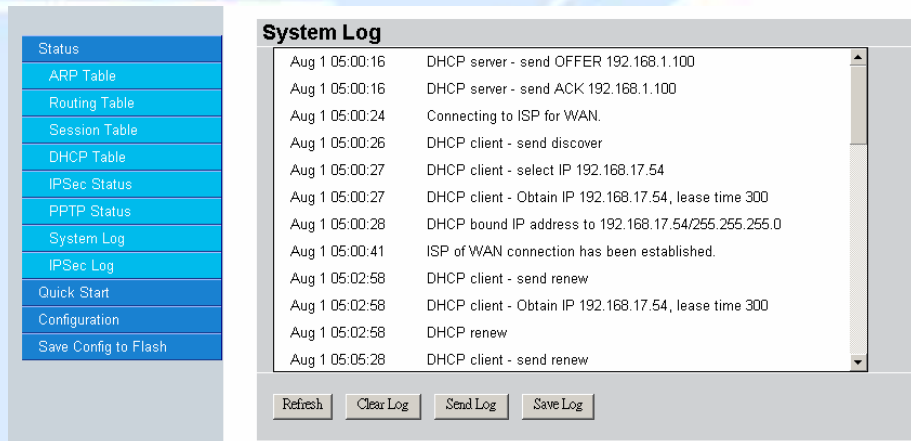
Peer Network: The Remote subnet for LAN to LAN as connection type.

Connect by: The remote address when connected.

Action: Manually drop the tunnel.

4.2.7 System Log

This window displays BiGuard 2/10's System Log entries. Major events are logged on this window.



Refresh: Refresh the System Log.

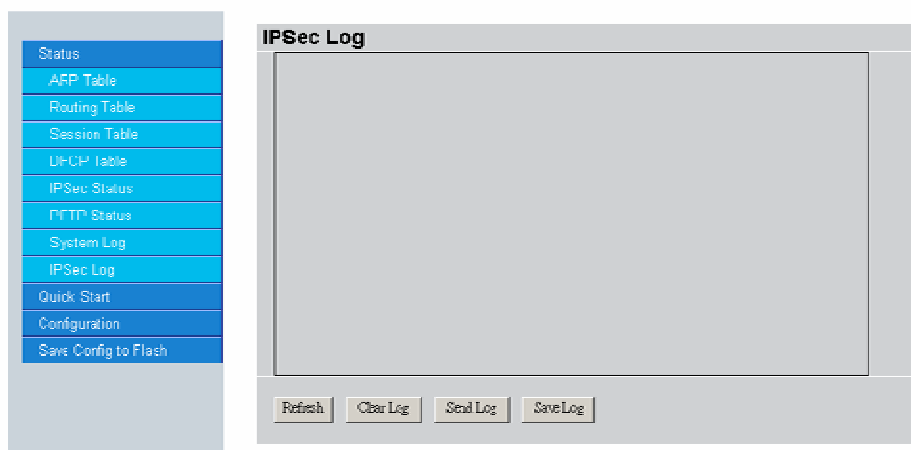
Clear Log: Clear the System Log.

Send Log: Send the System Log to your email account. You can set the email address in **Configuration > System > Email Alert**. See the **Email Alert** section for more details.

Save Log: Save the System log to a text file.

4.2.8 IPsec Log

This page displays the router's IPsec Log entries. Major events are logged to this window.



Refresh: Refresh the IPsec Log.

Clear Log: Clear the IPsec Log.

Send Log: Send IPsec Log to your email account. You can set the email address in **Configuration > System > Email Alert**. See the **Email Alert** section for more

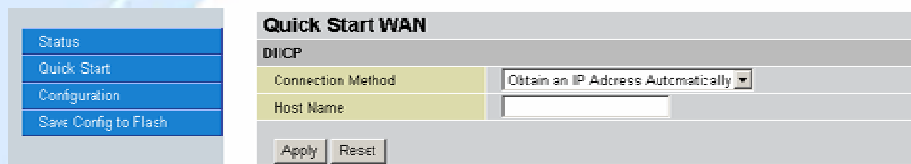
details.

Save Log: Save the IPsec log to a text file.

Please refer to *Appendix F: IPsec Log Events* for more information on log events.

4.3 Quick Start

The Quick Start menu allows you to quickly configure your network for Internet access using the most basic settings.

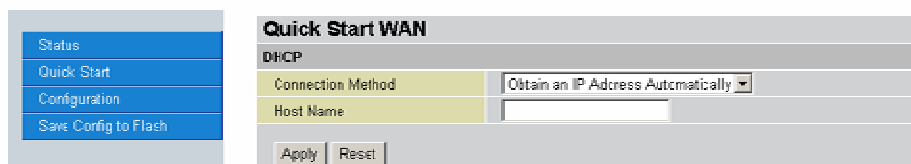


The screenshot shows the 'Quick Start WAN' configuration page. On the left is a navigation menu with 'Quick Start' selected. The main content area is titled 'Quick Start WAN' and has a sub-section 'DHCP'. It contains a 'Connection Method' dropdown menu set to 'Obtain an IP Address Automatically' and a 'Host Name' text input field. At the bottom are 'Apply' and 'Reset' buttons.

Connection Method: Select your router's connection to the Internet. Selections include **Obtain an IP Address Automatically**, **Static IP Settings**, **PPPoE Settings**, **PPTP Settings**, and **Big Pond Settings**.

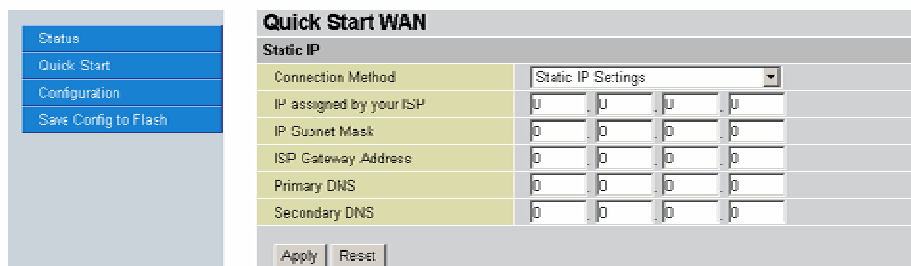
4.3.1 DHCP

The following is information regarding your ISP that you will need to enter in order to properly configure your Internet connection. If you select to **Obtain an IP Address Automatically**, these will be automatically set for you, provided that your ISP dynamically assigns an IP address.



This screenshot is identical to the one above, showing the 'Quick Start WAN' configuration page with the 'DHCP' section selected. The 'Connection Method' is 'Obtain an IP Address Automatically' and the 'Host Name' field is empty.

4.3.2 Static IP



The screenshot shows the 'Quick Start WAN' configuration page with the 'Static IP' section selected. The 'Connection Method' dropdown is set to 'Static IP Settings'. Below this are several input fields for IP addresses: 'IP assigned by your ISP', 'IP Subnet Mask', 'ISP Gateway Address', 'Primary DNS', and 'Secondary DNS'. Each field is a four-part numeric input (e.g., 0.0.0.0). At the bottom are 'Apply' and 'Reset' buttons.

IP assigned by your ISP: Enter the assigned IP address from your IP.

IP Subnet Mask: Enter your IP subnet mask.

ISP Gateway Address: Enter your ISP gateway address.

Primary DNS: Enter your primary DNS.

Secondary DNS: Enter your secondary DNS.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.3.3 PPPoE

Quick Start WAN	
PPPoE	
Connection Method	PPPoE Settings
Username	
Password	
Retype Password	
Connection	Always Connect
Idle Time	10 minutes
Apply Reset	

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.3.4 PPTP

The screenshot shows the 'Quick Start WAN' configuration page for PPTP. On the left is a navigation menu with 'Status', 'Quick Start', 'Configuration', and 'Save Config to Flash'. The main area is titled 'Quick Start WAN' and 'PPTP'. It contains the following fields:

Connection Method	PPTP Settings
Username	
Password	
Retype Password	
PPTP Client IP	0 0 0 0
PPTP Client IP Netmask	0 0 0 0
PPTP Client IP Gateway	0 0 0 0
PPTP Server IP	0 0 0 0
Connection	Always Connect
Idle Time	10 minutes

At the bottom are 'Apply' and 'Reset' buttons.

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

PPTP Client IP: Enter the PPTP Client IP provided by your ISP.

PPTP Client IP Netmask: Enter the PPTP Client IP Netmask provided by your ISP.

PPTP Client IP Gateway: Enter the PPTP Client IP Gateway provided by your ISP.

PPTP Server IP: Enter the PPTP Server IP provided by your ISP.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPTP session when starting up and to automatically re-establish the PPTP session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPTP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.3.5 Big Pond

The screenshot shows the 'Quick Start WAN' configuration page for Big Pond. On the left is a navigation menu with 'Status', 'Quick Start', 'Configuration', and 'Save Config to Flash'. The main area is titled 'Quick Start WAN' and 'Big Pond'. It contains the following fields:

Connection Method	Big Pond Settings
Username	
Password	
Retype Password	
Login server	0 0 0 0

At the bottom are 'Apply' and 'Reset' buttons.

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Login Server: Enter the IP of the Login server provided by your ISP.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

For detailed instructions on configuring WAN settings, please refer to the **WAN** section of this chapter.

4.4 Configuration

The **Configuration** menu allows you to set many of the operating parameters of the BiGuard 2/10. In this menu, you will find the following sections:

- LAN
- WAN
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced

These items are described below in the following sections.

Status Refresh

Device Information

Device Name	BiGuard2
System Up Time	0: 0:15:49 (day:hour:min:sec)
Current Time	Mon May 29 10:54:44 2006 Sync Now
Private LAN MAC Address	00:12:31:23:21:40
Public WAN MAC Address	00:04:ed:23:21:41
Firmware Version	1.05
Home URL	Billion Electric Co., Ltd.

LAN

IP Address	192.168.1.254
Netmask	255.255.255.0
DHCP Server	Enabled

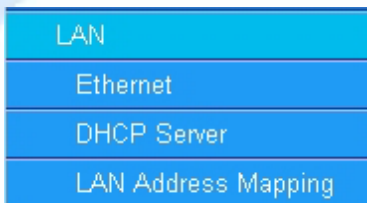
WAN

Connection Method	Connect by Static IP Settings
IP Address	192.168.17.109
Netmask	255.255.255.0
Gateway	192.168.17.70
DNS	192.168.0.219
Up Time	0: 0:15: 3 (day:hour:min:sec)

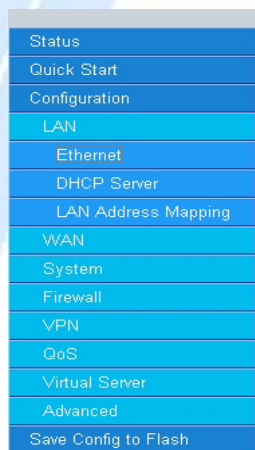
SAVE CONFIG RESTART LOGOUT

4.4.1 LAN

There are two items within this section: **Ethernet** ,**DHCP Server** and **LAN Address Mapping**.



4.4.1.1 Ethernet



Ethernet				
Parameters				
IP Address	192	168	1	254
Subnet Mask	255	255	255	0
RIP	Disable	<input checked="" type="radio"/> RIP-2B	<input type="radio"/> RIP-2M	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>				

IP Address: Enter the internal LAN IP address for BiGuard 2/10 (192.168.1.254 by default).

Subnet Mask: Enter the subnet mask (255.255.255.0 by default).

RIP: RIP v2 Broadcast and RIP v2 Multicast. Check to enable RIP.

4.4.1.2 DHCP Server

In this menu, you can disable or enable the Dynamic Host Configuration Protocol (DHCP) server. The DHCP protocol allows your BiGuard 2/10 to dynamically assign IP addresses to PCs on your network if they are configured to automatically obtain IP addresses.

- Status
- Quick Start
- Configuration
- LAN
 - Ethernet
 - DHCP Server
 - LAN Address Mapping
- WAN
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

DHCP Server

Parameters

DHCP Server Functions Enable Disable

IP Pool Range From 192.168.1.100

IP Pool Range to 192.168.1.199

Primary DNS Server

Secondary DNS Server

Primary WINS Server

Secondary WINS Server

Domain Name

[Fixed Host](#)

To disable the router's DHCP Server, select the **Disable** radio button, and then click **Apply**. When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (192.168.1.254 by default).

To configure the router's DHCP Server, select the **Enable** radio button, and then configure parameters of the DHCP Server including the IP Pool (starting IP address and ending IP address to be allocated to the PCs on your network), DNS Server, WINS Server, and Domain Name. These details are sent to each DHCP client when they request an IP address from the DHCP server. Click **Apply** to enable this function.

Fixed Host allows specific computer/network clients to have a reserved IP address.

- Status
- Quick Start
- Configuration
- LAN
 - Ethernet
 - DHCP Server
 - LAN Address Mapping
- WAN
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Fixed Host

Fixed Host Table

No.	MAC Address	IP Address
Create		

IP Address: Enter the IP address that you want to reserve for the above MAC address.

MAC Address: Enter the MAC address of the PC or server you wish to be assigned a

reserved IP.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

Status	Fixed Host
Quick Start	Create
Configuration	IP Address Candidates ▶ 192.168.1.0
LAN	MAC Address [] - [] - [] - [] - [] - []
Ethernet	<input type="button" value="Apply"/>
DHCP Server	
LAN Address Mapping	
WAN	
System	
Firewall	
VPN	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

Click the **Apply** button to add the configuration into the Host Table. Press the **Delete** button to delete a configuration from the Host Table.

4.4.1.3 LAN Address Mapping

LAN Address Mapping is a function that can support multiple subnet and also multiple NAT, you can specify a subnet and LAN Gateway IP Address and select associated WAN IP Address specified in WAN IP Alias in **Configuration -> WAN -> WAN IP Alias**.

Status	LAN Address Mapping
Quick Start	LAN Address Mapping Table
Configuration	NO. Name IP Address Netmask WAN IP
LAN	<input type="button" value="Create"/> ▶
Ethernet	
DHCP Server	
LAN Address Mapping	
WAN	
System	
Firewall	
VPN	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

Please click Create to create a LAN Address Mapping rule.

Status	LAN Address Mapping			
Quick Start	Add Subnet			
Configuration	Name	<input type="text"/>		
LAN	IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>
Ethernet	Netmask	<input type="text"/>	<input type="text"/>	<input type="text"/>
DHCP Server	WAN IP Address Candidates ▶	<input type="text"/>	<input type="text"/>	<input type="text"/>
LAN Address Mapping	<input type="button" value="Apply"/>			
WAN				
System				
Firewall				
VPN				
QoS				
Virtual Server				
Advanced				
Save Config to Flash				

Name: Please input the name of the rule.

IP Address: Please input the LAN Gateway IP Address you would like to use.

Netmask: Please input the Netmask you would like to use.

WAN IP Address: Please click Candidates to select the WAN IP address you would like to use from WAN Alias list.

Click the **Apply** button to add the configuration into the LAN Address Mapping.

4.4.2 WAN

WAN refers to your Wide Area Network connection. In most cases, this means your router's connection to the Internet through your ISP. There are three items within this section:

- WAN
- WAN
- Bandwidth Settings
- WAN IP Alias

4.4.2.1 WAN

Status	WAN	
Quick Start	DHCP	
Configuration	Connection Method	Obtain an IP Address Automatically ▾
LAN	Host Name	Obtain an IP Address Automatically
WAN	MAC Address	Static IP Settings
WAN	Candidates ▶	PPPoE Settings
Bandwidth Settings		PPTP Settings
WAN IP Alias		Big Pond Settings
System	DNS	<input type="checkbox"/> Your ISP requires you to manually setup DNS settings
Firewall	Primary DNS	0 . 0 . 0 . 0
VPN	Secondary DNS	0 . 0 . 0 . 0
QoS	RIP	Disable ▾ <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
Virtual Server	MTU	1500
Advanced	Ethernet MAC: . 00 . 00 . 00	
Save Config to Flash	Apply Reset	

Connection Method: Select how your router will connect to the Internet. Selections include **Obtain an IP Address Automatically**, **Static IP Settings**, **PPPoE Settings**, **PPTP Settings**, and **Big Pond Settings**. For each WAN port, the factory default is DHCP. If your ISP does not use DHCP, select the correct connection method and configure the connection accordingly. Configurable items will vary depending on the connection method selected.

4.4.2.1.1 DHCP

Status	WAN	
Quick Start	DHCP	
Configuration	Connection Method	Obtain an IP Address Automatically ▾
LAN	Host Name	
WAN	MAC Address	<input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
WAN	Candidates ▶	MAC Address: 00 . 00 . 00 . 00 . 00 . 00
Bandwidth Settings	DNS	<input type="checkbox"/> Your ISP requires you to manually setup DNS settings
WAN IP Alias	Primary DNS	0 . 0 . 0 . 0
System	Secondary DNS	0 . 0 . 0 . 0
Firewall	RIP	Disable ▾ <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
VPN	MTU	1500
QoS	Apply Reset	
Virtual Server		
Advanced		
Save Config to Flash		

Host Name: Some ISPs authenticate logins using this field.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

Candidates: You can also select the MAC address from the list in the Candidates.

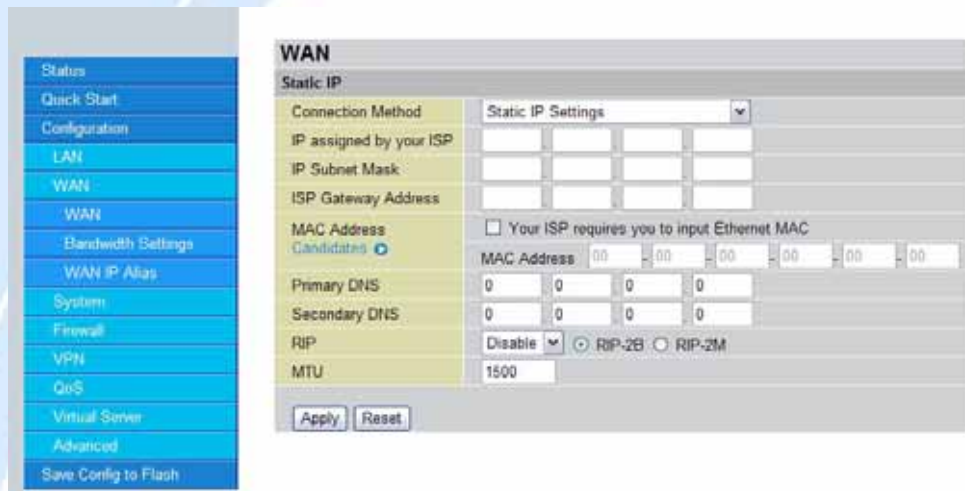
DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.4.2.1.2 Static IP



IP assigned by your ISP: Enter the static IP assigned by your ISP.

IP Subnet Mask: Enter the IP subnet mask provided by your ISP.

ISP Gateway Address: Enter the ISP gateway address provided by your ISP.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

Candidates: You can also select the MAC address from the list in the Candidates.

Primary DNS: Enter the primary DNS provided by your ISP.

Secondary DNS: Enter the secondary DNS provided by your ISP.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.4.2.1.3 PPPoE

Status	WAN
Quick Start	PPPoE
Configuration	Connection Method <input type="text" value="PPPoE Settings"/>
LAN	Username <input type="text"/>
WAN	Password <input type="text"/>
WAN	Retype Password <input type="text"/>
Bandwidth Settings	Connection <input type="text" value="Always Connect"/>
WAN IP Alias	Idle Time <input type="text" value="10 minutes"/>
System	<input checked="" type="radio"/> Dynamic (IP automatically assigned by your ISP)
Firewall	<input type="radio"/> Fixed (Your ISP requires you to input IP address)
VPN	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
QoS	<input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
Virtual Server	MAC Address <input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/> - <input type="text" value="00"/>
Advanced	<input type="checkbox"/> Your ISP requires you to manually setup DNS settings
Save Config to Flash	DNS
	Primary DNS <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
	Secondary DNS <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
	RIP <input type="text" value="Disable"/> <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
	MTU <input type="text" value="1492"/>
	<input type="button" value="Apply"/> <input type="button" value="Reset"/>

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

IP Assigned by your ISP: If your IP is dynamically assigned by your ISP, select the **Dynamic** radio button. If your IP assigns a static IP address, select the **Static** radio button, and input your IP address in the blank provided.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

Candidates: You can also select the MAC address from the list in the Candidates.

DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.
Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.4.2.1.4 PPTP

WAN	
PPTP	
Connection Method	PPTP Settings
Username	
Password	
Retype Password	
PPTP Client IP	0 0 0 0
PPTP Client IP Netmask	0 0 0 0
PPTP Client IP Gateway	0 0 0 0
PPTP Server IP	0 0 0 0
Connection	Always Connect
Idle Time	10 minutes
IP assigned by your ISP	<input checked="" type="radio"/> Dynamic (IP automatically assigned by your ISP) <input type="radio"/> Fixed (Your ISP requires you to input IP address)
MAC Address	<input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
MAC Address Candidates	MAC Address 00 00 00 00 00 00
DNS	<input type="checkbox"/> Your ISP requires you to manually setup DNS settings
Primary DNS	0 0 0 0
Secondary DNS	0 0 0 0
RIP	Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
MTU	1432
Apply Reset	

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

PPTP Client IP: Enter the PPTP Client IP provided by your ISP.

PPTP Client IP Netmask: Enter the PPTP Client IP Netmask provided by your ISP.

PPTP Client IP Gateway: Enter the PPTP Client IP Gateway provided by your ISP.

PPTP Server IP: Enter the PPTP Server IP provided by your ISP.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPTP session when starting up and to automatically re-establish the PPTP session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPTP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

IP Assigned by your ISP: If your IP is dynamically assigned by your ISP, select the **Dynamic** radio button. If your IP assigns a static IP address, select the **Static** radio button. This will take you to another page for inputting the IP address information.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

Candidates: You can also select the MAC address from the list in the Candidates.

DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send, Receive,** or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.4.2.1.5 Big Pond

WAN	
Big Pond	
Connection Method	Big Pond Settings
Username	
Password	
Retype Password	
Login server	0 . 0 . 0 . 0
MAC Address	<input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
Candidates	MAC Address 00 . 00 . 00 . 00 . 00 . 00
DNS	<input type="checkbox"/> Your ISP requires you to manually setup DNS settings
	Primary DNS 0 . 0 . 0 . 0
	Secondary DNS 0 . 0 . 0 . 0
RIP	Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
MTU	1500
Apply Reset	

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Login Server: Enter the IP of the Login server provided by your ISP.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

Candidates: You can also select the MAC address from the list in the Candidates.

DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send, Receive,** or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

A simpler alternative is to select **Quick Start** from the main menu. Please see the **Quick Start** section of this chapter for more information.

4.4.2.2 Bandwidth Settings

Under Bandwidth Settings, you can easily configure both inbound and outbound bandwidth.

Bandwidth Settings			
Max Bandwidth Provided by ISP			
WAN	Outbound Bandwidth	<input type="text" value="102400"/>	kbps
	Inbound Bandwidth	<input type="text" value="102400"/>	kbps
<input type="button" value="Apply"/>			

WAN: Enter your ISP inbound and outbound bandwidth for WAN.

NOTE: These values entered here are referenced by QoS.

4.4.2.3 WAN IP Alias

WAN IP Alias allows you to input additional WAN IP addresses. WAN IP Alias can be used for Multiple NAT settings, including LAN Address Mapping settings and Virtual Server settings.

- Status
- Quick Start
- Configuration
- LAN
- WAN
- WAN
- Bandwidth Settings
- WAN IP Alias
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

WAN IP Alias

WAN IP Alias Table

NO.	Name	IP Address		
Create				

Please click Create to create a LAN Address Mapping rule.

- Status
- Quick Start
- Configuration
- LAN
- WAN
- WAN
- Bandwidth Settings
- WAN IP Alias
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

WAN IP Alias

Add WAN IP

Name	<input type="text"/>
IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<input type="button" value="Apply"/>	

Name: Please input the name of the rule.

IP Address: Please input the additional WAN IP address you would like to use.

Click the **Apply** button to add the configuration into the WAN IP Alias.

4.4.3 System

The System menu allows you to adjust a variety of basic router settings, upgrade firmware, set up remote access, and more. In this menu are the following sections: Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart, Password, System Log Server and Email Alert.

- System
- Time Zone
- Remote Access
- Firmware Upgrade
- Backup / Restore
- Restart
- Password
- System Log Server
- E-Mail Alert

4.4.3.1 Time Zone

BiGuard 2/10 does not use an onboard real time clock; instead, it uses the Network Time Protocol (NTP) to acquire the current time from an NTP server outside your network. Simply choose your local time zone, enter NTP Server IP Address, and click **Apply**. After connecting to the Internet, BiGuard 2/10 will retrieve the correct local time from the NTP server you have specified. Your ISP may provide an NTP server for you to use.

Time Zone	
Parameters	
Time Zone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Local Time Zone (+GMT Time)	(GMT-07:00)Mountain Time (US & Canada)
NTP Server Address	caif.css.gov india.colorado.edu time.nist.gov time-b.nist.gov
Daylight Saving	<input type="checkbox"/> Automatic
Resync Period	1440 minutes

Time Zone: Select Enable or Disable this function.

Local Time Zone(+GMT Time): Please select the time zone that belongs to your area.

NTP Server Address: Please input the NTP server address you would like to use.

Daylight Saving: To have BiGuard 2/10 automatically adjust for Daylight Savings

Time, please check the **Automatic** checkbox.

Resync Period: Please input the resync circle of time zone update.

Click Apply to apply the rule, Click Cancel to discard the changes.

4.4.3.2 Remote Access

To allow remote users to configure and manage BiGuard 2/10 through the Internet, select the Enable radio button. To deactivate remote access, select the **Disable** radio button. This function also enables you grant access from any PC or from a specific IP address. Click **Apply** to save your settings.

NOTE: When enabling remote access, be sure to change the default administration password to something more secure.

The screenshot shows the router's configuration menu on the left and the Remote Access configuration page on the right. The menu includes: Status, Quick Start, Configuration, LAN, WAN, System, Time Zone, Remote Access, Firmware Upgrade, Backup / Restore, Restart, Password, System Log Server, E-Mail Alert, Firewall, VPN, QoS, Virtual Server, Advanced, and Save Config to Flash. The Remote Access page has a 'Remote Access Function' section with an 'Action' field containing radio buttons for 'Enable' and 'Disable' (selected). Below it is an '* HTTPS Port' field with the value '443'. A note states: '* : This setting will become effective after you save to flash and restart the router.' An 'Apply' button is at the bottom. Below this is a 'Remote Access Table' section with a table header: 'No.', 'IP Address', and two empty columns. A 'Create' button with a right-pointing arrow is below the table.

Action: Select Enable or Disable remote access function.

HTTPS Port: Please input the remote access HTTPS port you would like to use.(default is 443)

Click Apply to apply your settings.

Click Create to add a Remote Access Table to specify the allowed remote access addresses.

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Time Zone
- Remote Access
- Firmware Upgrade
- Backup / Restore
- Restart
- Password
- System Log Server
- E-Mail Alert
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Remote Access

You may permit remote administration of this network device (HTTPS).

Allow Remote Access By

Everyone (Change default password!)
 Only this PC: . . .
 PC from this subnet:
 . . .

Apply

Allow Remote Access By:

Everyone: Please check if you allow any IP addresses for the remote user to access.

Only the PC: Please specify the IP Address that is allowed to access.

PC from the subnet: Please specify the subnet that is allowed to access.

4.4.3.3 Firmware Upgrade

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Time Zone
- Remote Access
- Firmware Upgrade
- Backup / Restore
- Restart
- Password
- System Log Server
- E-Mail Alert
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Firmware Upgrade

You may upgrade the system software on your network device

New Firmware Image 瀏覽...

Upgrade

Upgrading your BiGuard 2/10's firmware is a quick and easy way to enjoy increased functionality, better reliability, and ensure trouble-free operation. To upgrade your firmware, simply visit Billion's website (<http://www.billion.com>) and download the latest firmware image file for BiGuard 2/10. Next, click **Browse** and select the newly downloaded firmware file. Click **Upgrade** to complete the update.

NOTE: DO NOT power down the router or interrupt the firmware upgrade while it is still in process. Interrupting the firmware upgrade process could damage the router.

4.4.3.4 Backup / Restore

Backup/Restore
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration
Backup configuration to your computer.

Restore Configuration
Configuration File
"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

This feature allows you to save and backup your router's current settings, or restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

To backup your router's settings, click **Backup** and select where to save the settings backup file. You may also change the name of the file when saving if you wish to keep multiple backups. Click **OK** to save the file.

To restore a previously saved backup file, click **Browse**. You will be prompted to

select a file from your PC to restore. Be sure to only restore setting files that have been generated by the Backup function, and that were created when using the same firmware version. Settings files saved to your PC should not be manually edited in any way. After selecting the settings file you wish to use, clicking **Restore** will load those settings into the router.

4.4.3.5 Restart

Status	Restart After restarting. Please wait for several seconds to let the system restart Restart Router with <input checked="" type="radio"/> Current Settings <input type="radio"/> Factory Default Settings <input type="button" value="Restart"/>
Quick Start	
Configuration	
LAN	
WAN	
System	
Time Zone	
Remote Access	
Firmware Upgrade	
Backup / Restore	
Restart	
Password	
System Log Server	
E-Mail Alert	
Firewall	
VPN	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

The Restart feature allows you to easily restart BiGuard 2/10. To restart with your last saved configuration, select the **Current Settings** radio button and click **Restart**.

If you wish to restart the router using the factory default settings, select **Factory Default Settings** and click **Restart** to reboot BiGuard 2/10 with factory default settings.

You may also reset your router to factory default settings by holding the Reset button on the router until the Status LED begins to blink. Once BiGuard 2/10 completes the boot sequence, the Status LED will stop blinking.

4.4.3.6 Password

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
 - Time Zone
 - Remote Access
 - Firmware Upgrade
 - Backup / Restore
 - Restart
 - Password
 - System Log Server
 - E-Mail Alert
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Password

Parameters

Password	*****
Confirm	*****

! Note: number of maximum characters of password is 32 characters.

Apply Reset

In order to prevent unauthorized access to your router's configuration interface, it requires the administrator to login with a password. You can change your password by entering your new password in both fields. Click **Apply** to save your changes. Click **Reset** to reset to the default administration password (admin).

4.4.3.7 System Log Server

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
 - Time Zone
 - Remote Access
 - Firmware Upgrade
 - Backup / Restore
 - Restart
 - Password
 - System Log Server
 - E-Mail Alert
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

System Log Server

Parameters

Send Log To Remote Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Log Server IP Address	192 . 168 . 1 . 1

Apply

This function allows BiGuard 2/10 to send system logs to an external Syslog Server. Syslog is an industry-standard protocol used to capture information about network activity. To enable this function, select the **Enable** radio button and enter your Syslog server IP address in the **Log Server IP Address** field. Click **Apply** to save your changes.

To disable this feature, simply select the **Disable** radio button and click **Apply**.

4.4.3.8 E-mail Alert

Status	<h4>E-Mail Alert</h4> <p>Parameters</p> <table border="1"> <tr> <td>E-Mail Alert</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>Recipient's E-Mail Address</td> <td><input type="text"/></td> </tr> <tr> <td>Sender's E-Mail Address</td> <td><input type="text"/></td> </tr> <tr> <td>SMTP Mail Server</td> <td><input type="text"/></td> </tr> <tr> <td>Mail Server Login</td> <td><input type="radio"/> Enable <input checked="" type="radio"/> Disable</td> </tr> <tr> <td>Username</td> <td><input type="text"/></td> </tr> <tr> <td>Password</td> <td><input type="password"/></td> </tr> <tr> <td rowspan="5">Alert via E-Mail when</td> <td><input type="radio"/> Immediately</td> </tr> <tr> <td><input type="radio"/> Hourly</td> </tr> <tr> <td><input type="radio"/> Daily <input type="text" value="12:00"/> <input checked="" type="radio"/> A.M. <input type="radio"/> P.M.</td> </tr> <tr> <td><input type="radio"/> Weekly <input type="text" value="Sunday"/></td> </tr> <tr> <td><input checked="" type="radio"/> When log is full</td> </tr> </table> <p style="text-align: center;"><input type="button" value="Apply"/></p>	E-Mail Alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Recipient's E-Mail Address	<input type="text"/>	Sender's E-Mail Address	<input type="text"/>	SMTP Mail Server	<input type="text"/>	Mail Server Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Username	<input type="text"/>	Password	<input type="password"/>	Alert via E-Mail when	<input type="radio"/> Immediately	<input type="radio"/> Hourly	<input type="radio"/> Daily <input type="text" value="12:00"/> <input checked="" type="radio"/> A.M. <input type="radio"/> P.M.	<input type="radio"/> Weekly <input type="text" value="Sunday"/>	<input checked="" type="radio"/> When log is full
E-Mail Alert		<input type="radio"/> Enable <input checked="" type="radio"/> Disable																			
Recipient's E-Mail Address		<input type="text"/>																			
Sender's E-Mail Address		<input type="text"/>																			
SMTP Mail Server		<input type="text"/>																			
Mail Server Login		<input type="radio"/> Enable <input checked="" type="radio"/> Disable																			
Username		<input type="text"/>																			
Password		<input type="password"/>																			
Alert via E-Mail when		<input type="radio"/> Immediately																			
		<input type="radio"/> Hourly																			
		<input type="radio"/> Daily <input type="text" value="12:00"/> <input checked="" type="radio"/> A.M. <input type="radio"/> P.M.																			
		<input type="radio"/> Weekly <input type="text" value="Sunday"/>																			
		<input checked="" type="radio"/> When log is full																			
Quick Start																					
Configuration																					
LAN																					
WAN																					
System																					
Time Zone																					
Remote Access																					
Firmware Upgrade																					
Backup / Restore																					
Restart																					
Password																					
System Log Server																					
E-Mail Alert																					
Firewall																					
VPN																					
QoS																					
Virtual Server																					
Advanced																					
Save Config to Flash																					

The Email Alert function allows a log of security-related events (such as System Log and IPSec Log) to be sent to a specified email address.

Email Alert: You may enable or disable this function by selecting the appropriate radio button.

Recipient's Email Address: Enter the email address where you wish the alert logs to be sent.

SMTP Mail Server: Enter your email account's outgoing mail server. It may be an IP address or a domain name.

Sender's Email Address: Enter the email address where you wish the alert logs to be sent by which address.

Mail Server Login: some SMTP servers may request users to login before serving.

Select **Enable** to activate SMTP server login function, **disable** to deactivate.

Username: Input the SMTP server's username.

Password: Input the SMTP server's password.

Alert via Email when: Select the frequency of each email update. Choose one of the five options:

Immediately: The router will send an alert immediately.

Hourly: The router will send an alert once every hour.

Daily: The router will send an alert once a day. The exact time can be specified using the pull down menu.

Weekly: The router will send an alert once a week.

When log is full: The router will send an alert only when the log is full.

4.4.4 Firewall

BiGuard 2/10 includes a full Stateful Packet Inspection (SPI) firewall for controlling Internet access from your LAN, and preventing attacks from hackers. Your router also acts as a "natural" Internet firewall when using Network Address Translation (NAT), as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet. Please see the WAN configuration section for more details.

Firewall
Packet Filter
URL Filter
LAN MAC Filter
Block WAN Request
Intrusion Detection

You can find five items under the Firewall section: **Packet Filter**, **URL Filter**, **LAN MAC Filter**, **Block WAN Request** and **Intrusion Detection**.

4.4.4.1 Packet Filter

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Firewall
 - Packet Filter
 - URL Filter
 - LAN MAC Filter
 - Block WAN Request
 - Intrusion Detection
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Packet Filter

Packet Filter Table									
ID	Enable	Action	Direction	Src. IP	Dest. IP	Protocol	Src. Port	Dest. Port	
Create ▶									

The Packet Filter function is used to limit user access to certain sites on the Internet or LAN. The Filter Table displays all current filter rules. If there is an entry in the Filter Table, you can click **Edit** to modify the setting of this entry, or click **Delete** to remove this entry, or click **Move** to change this entry's priority. When the entry is upper, the priority is higher.

To create a new filter rule, click **Create**.

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Firewall
 - Packet Filter
 - URL Filter
 - LAN MAC Filter
 - Block WAN Request
 - Intrusion Detection
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Packet Filter

Add Filtering Rules

ID	1		
Rule	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Action When Matched	Drop		
Direction	Outgoing		
Source IP	Any	Start IP Address	0 0 0 0
		End IP Address	0 0 0 0
		Netmask	0 0 0 0
Destination IP	Any	Start IP Address	0 0 0 0
		End IP Address	0 0 0 0
		Netmask	0 0 0 0
Protocol	Any		
Source Port Range	1	-5535	
Destination Port Range	1	-5535	

Apply

- ID: This is an identify that allows you to move the rule by before or after an ID.
- Rule: Enable or Disable this entry.
- Action When Matched: Select to **Drop** or **Forward** the packet specified in this filter entry.
- Direction: Incoming Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet. Outgoing Packet Filter

rules prevent unauthorized computers or applications accessing the Internet. Select if the new filter rule is incoming or outgoing.

Source IP: Select **Any**, **Subnet**, **IP Range** or **Single Address**.

Starting IP Address: Enter the source IP or starting source IP address this filter rule is to be applied.

End IP Address: Enter the End source IP Address this filter rule is to be applied. (for IP Range only)

Netmask: Enter the subnet mask of the above IP address.

Destination IP: Select **Any**, **Subnet**, **IP Range** or **Single Address**.

Starting IP Address: Enter the destination IP or starting destination IP address this filter rule is to be applied.

End IP Address: Enter the End destination IP Address this filter rule is to be applied. (for IP Range only)

Netmask: Enter the subnet mask of the above IP address.

Protocol: Select the Transport protocol type (Any, TCP, UDP).

Source Port Range: Enter the source port number range. If you only want to specify one service port, then enter the same port number in both boxes.

Destination Port Range: Enter the destination port number range. If you only want to specify one service port, then enter the same port number in both boxes.

Helper: You could also select the application type you would like to apply for automatic input.

4.4.4.2 URL Filter

Status	URL Filter		
Quick Start	Configuration		
Configuration	URL Filtering	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
LAN	Keyword Filtering	<input type="checkbox"/> Enable Details	
WAN	Domains Filtering	<input type="checkbox"/> Enable Details	
System		<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains	
Firewall	Restrict URL Features	<input type="checkbox"/> Block Java Applet	
Packet Filter		<input type="checkbox"/> Block ActiveX	
URL Filter		<input type="checkbox"/> Block Web proxy	
LAN MAC Filter		<input type="checkbox"/> Block Cookie	
Block WAN Request		<input type="checkbox"/> Block Surfing by IP Address	
Intrusion Detection	<input type="button" value="Apply"/>		
VPN	Exception List		
QoS	Name	IP Address	
Virtual Server	<input type="button" value="Create"/>		
Advanced			
Save Config to Flash			

The URL Filter is a powerful tool that can be used to limit access to certain URLs on the Internet. You can block web sites based on keywords or even block out an entire domain. Certain web features can also be blocked to grant added security to your network.

URL Filtering: You can choose to Enable or Disable this feature.

Keyword Filtering: Click the checkbox to enable this feature. To edit the list of filtered keywords, click Details.

Domain Filtering: Click the "enable" checkbox to enable filtering by Domain Name. Click the "Disable all WEB traffic except for trusted domains" check box to allow web access only for trusted domains.

Restrict URL Features: Click "Block Java Applet" to filter web access with Java Applet components. Click "Block ActiveX" to filter web access with ActiveX components. Click "Block Web proxy" to filter web proxy access. Click "Block Cookie" to filter web access with Cookie components. Click "Block Surfing by IP Address" to filter web access with an IP address as the domain name.

Exception List: You can input a list of IP addresses as the exception list for URL filtering.

Status
Quick Start
Configuration
LAN
WAN
System
Firewall
Packet Filter
URL Filter
LAN MAC Filter
Block WAN Request
Intrusion Detection
VPN
QoS
Virtual Server
Advanced
Save Config to Flash

Keywords Filtering

Create

Keyword

Block WEB URLs which contain these keywords

No.	Keyword
-----	---------

Enter a keyword to be filtered and click **Apply**. Your new keyword will be added to the filtered keyword listing.

Domains Filtering: Click the top checkbox to enable this feature. You can also choose to disable all web traffic except for trusted sites by clicking the bottom

checkbox. To edit the list of filtered domains, click **Details**.

Status	Domains Filtering	
Quick Start	Create	
Configuration	Domain Name	<input type="text"/>
LAN	Type	Forbidden Domain ▾
WAN	<input type="button" value="Apply"/>	
System	Trusted Domain Table	
Firewall	No.	Domain
Packet Filter	Forbidden Domain Table	
URL Filter	No.	Domain
LAN MAC Filter		
Block WAN Request		
Intrusion Detection		
VPN		
QoS		
Virtual Server		
Advanced		
Save Config to Flash		

Enter a domain and selected whether this domain is trusted or forbidden with the pull-down menu. Next, click **Apply**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously.

Restrict URL Features: Use this to disable certain web features. Select the options you want (Block Java Applet, Block ActiveX, Block Web proxy, Block Cookie, Block Surfing by IP Address) and click **Apply** to save your changes.

You may also designate which IP addresses are to be excluded from these filters by adding them to the Exception List. To do so, click **Add**.

Status
Quick Start
Configuration
LAN
WAN
System
Firewall
Packet Filter
URL Filter
LAN MAC Filter
Block WAN Request
Intrusion Detection
VPN
QoS
Virtual Server
Advanced
Save Config to Flash

Exception

Create

Name	<input type="text"/>
IP Address Candidates ▶	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Enter a name for the IP Address and then enter the IP address itself. Click **Apply** to save your changes. The IP address will be entered into the Exception List, and excluded from the URL filtering rules in effect.

4.4.4.3 LAN MAC Filter

Status
Quick Start
Configuration
LAN
WAN
System
Firewall
Packet Filter
URL Filter
LAN MAC Filter
Block WAN Request
Intrusion Detection
VPN
QoS
Virtual Server
Advanced
Save Config to Flash

LAN MAC Filter

Default Rule

Action	<input checked="" type="radio"/> Forward <input type="radio"/> Drop
--------	---

Rule Lists

No.	Enable	Action	MAC Address	
Create ▶				

LAN Mac Filter can decide that BiGuard will serve those devices at LAN side or not by MAC Address.

Default Rule: Forward or Drop all LAN requests. (Forward by default)

Create: You can also input a specified MAC Address to be dropped or Forward without depending on the default rule.

Status	<h2>LAN MAC Filter</h2> <p>Create Rule</p> <table border="1"> <tr> <td>Rule</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td>Action When Matched</td> <td>Drop</td> </tr> <tr> <td>Mac Address</td> <td>Candidates ▶ <input type="text"/></td> </tr> <tr> <td colspan="2"><input type="button" value="Apply"/></td> </tr> </table>	Rule	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Action When Matched	Drop	Mac Address	Candidates ▶ <input type="text"/>	<input type="button" value="Apply"/>	
Rule		<input checked="" type="radio"/> Enable <input type="radio"/> Disable							
Action When Matched		Drop							
Mac Address		Candidates ▶ <input type="text"/>							
<input type="button" value="Apply"/>									
Quick Start									
Configuration									
LAN									
WAN									
System									
Firewall									
Packet Filter									
URL Filter									
LAN MAC Filter									
Block WAN Request									
Intrusion Detection									
VPN									
QoS									
Virtual Server									
Advanced									
Save Config to Flash									

Rule: Enable or disable this entry.

Action When Matched: Select to **Drop** or **Forward** the packet specified in this filter entry.

MAC Address: The MAC Address you would like to apply.

Candidates: You can also select the **Candidates** which are referred from the ARP table for automatic input.

4.4.4.4 Block WAN Request

Status	<h2>Block WAN Request</h2> <p>Enable for preventing any ping test from Internet, such as hacker attack.</p> <table border="1"> <tr> <td>Block WAN Request</td> <td><input checked="" type="radio"/> Enable <input type="radio"/> Disable</td> </tr> <tr> <td colspan="2"><input type="button" value="Apply"/></td> </tr> </table>	Block WAN Request	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="button" value="Apply"/>	
Block WAN Request		<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
<input type="button" value="Apply"/>					
Quick Start					
Configuration					
LAN					
WAN					
System					
Firewall					
Packet Filter					
URL Filter					
LAN MAC Filter					
Block WAN Request					
Intrusion Detection					
VPN					
QoS					
Virtual Server					
Advanced					
Save Config to Flash					

Blocking WAN requests is one way to prevent DDoS attacks by preventing ping requests from the Internet. Use this menu to enable or disable function.

4.4.4.5 Intrusion Detection

Status	Intrusion Detection
Quick Start	Enable for preventing hacker attack from Internet.
Configuration	Intrusion Detection <input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN	Intrusion Log <input type="radio"/> Enable <input checked="" type="radio"/> Disable
WAN	<input type="button" value="Apply"/>
System	
Firewall	
Packet Filter	
URL Filter	
LAN MAC Filter	
Block WAN Request	
Intrusion Detection	
VPN	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

Intrusion Detection can prevent most common DoS attacks from the Internet or from LAN users.

Intrusion Detection: Enable or disable this function.

Intrusion Log: All the detected and dropped attacks will be shown in the system log.

4.4.5 VPN

4.4.5.1 IPSec

IPSec is a set of protocols that enable Virtual Private Networks (VPN). VPN is a way to establish secured communication tunnels to an organization's network via the Internet.

4.4.5.1.1 IPSec Wizard

Status	<h2>IPSec Wizard</h2> <h3>Step 1 of 3: Connection Information</h3> <table border="1"> <tr> <td>Connection Name</td> <td><input type="text"/></td> </tr> <tr> <td>PreShared Key</td> <td><input type="text"/></td> </tr> <tr> <td rowspan="5">Connection Type</td> <td><input checked="" type="radio"/> LAN to LAN</td> </tr> <tr> <td><input type="radio"/> LAN to LAN (Mobile LAN)</td> </tr> <tr> <td><input type="radio"/> LAN to Host</td> </tr> <tr> <td><input type="radio"/> LAN to Host (Mobile Client)</td> </tr> <tr> <td><input type="radio"/> LAN to Host (For BiGuard VPN Client)</td> </tr> <tr> <td colspan="2"><input type="button" value="Next"/></td> </tr> </table>	Connection Name	<input type="text"/>	PreShared Key	<input type="text"/>	Connection Type	<input checked="" type="radio"/> LAN to LAN	<input type="radio"/> LAN to LAN (Mobile LAN)	<input type="radio"/> LAN to Host	<input type="radio"/> LAN to Host (Mobile Client)	<input type="radio"/> LAN to Host (For BiGuard VPN Client)	<input type="button" value="Next"/>	
Connection Name		<input type="text"/>											
PreShared Key		<input type="text"/>											
Connection Type		<input checked="" type="radio"/> LAN to LAN											
		<input type="radio"/> LAN to LAN (Mobile LAN)											
		<input type="radio"/> LAN to Host											
		<input type="radio"/> LAN to Host (Mobile Client)											
		<input type="radio"/> LAN to Host (For BiGuard VPN Client)											
<input type="button" value="Next"/>													
Quick Start													
Configuration													
LAN													
WAN													
System													
Firewall													
VPN													
IPSec													
IPSec Wizard													
IPSec Policy													
PPTP													
QoS													
Virtual Server													
Advanced													
Save Config to Flash													

Connection Name: A user-defined name for the connection.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Connection Type:

There are 5 connection types:

(1) LAN to LAN: BiGuard would like to establish an IPSec VPN tunnel with remote router using Fixed Internet IP or domain name by using main mode.

Status	<h2>IPSec Wizard</h2> <h3>Step 2 of 3: Remote Information</h3> <table border="1"> <tr> <td>Remote Secure Gateway Address (or Hostname)</td> <td colspan="4"><input type="text"/></td> </tr> <tr> <td rowspan="2">Remote Network</td> <td>IP Address</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>Netmask</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="6"><input type="button" value="Back"/> <input type="button" value="Next"/></td> </tr> </table>	Remote Secure Gateway Address (or Hostname)	<input type="text"/>				Remote Network	IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Netmask	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Back"/> <input type="button" value="Next"/>					
Remote Secure Gateway Address (or Hostname)		<input type="text"/>																					
Remote Network		IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																	
		Netmask	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																	
<input type="button" value="Back"/> <input type="button" value="Next"/>																							
Quick Start																							
Configuration																							
LAN																							
WAN																							
System																							
Firewall																							
VPN																							
IPSec																							
IPSec Wizard																							
IPSec Policy																							
PPTP																							
QoS																							
Virtual Server																							
Advanced																							
Save Config to Flash																							

Remote Secure Gateway Address (or HostName): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

Remote Network: The subnet of the remote network. Allows you to enter an IP address and netmask.

Back: Back to the Previous page.

Next: Go to the next page.

(2)LAN to LAN (Mobile LAN): BiGuard would like to establish an IPSec VPN tunnel with remote router using Dynamic Internet IP by using aggressive mode.

Status	IPSec Wizard Step 2 of 3: Remote Information Remote Identifier <input type="text"/> Remote Network IP Address <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> Netmask <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="button" value="Back"/> <input type="button" value="Next"/>
Quick Start	
Configuration	
LAN	
WAN	
System	
Firewall	
VPN	
IPSec	
IPSec Wizard	
IPSec Policy	
PPTP	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

Remote Identifier: The Identifier of remote gateway, all input value type will be auto-defined as IP Address, FQDN(DNS) or FQUN(E-mail).

Remote Network: The subnet of the remote network. Allows you to enter an IP address and netmask.

Back: Back to the Previous page.

Next: Go to the next page.

(3)LAN to Host: BiGuard would like to establish an IPSec VPN tunnel with remote client software using Fixed Internet IP or domain name by using main mode.

Status	IPSec Wizard Step 2 of 3: Remote Information Remote Secure Gateway Address (or Hostname) <input type="text"/> <input type="button" value="Back"/> <input type="button" value="Next"/>
Quick Start	
Configuration	
LAN	
WAN	
System	
Firewall	
VPN	
IPSec	
IPSec Wizard	
IPSec Policy	
PPTP	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

Remote Secure Gateway Address (or Hostname): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

Back: Back to the Previous page.

Next: Go to the next page.

(4)LAN to Host (Mobile Client): BiGuard would like to establish an IPSec VPN tunnel with remote client software using Dynamic Internet IP by using aggressive mode.


Status	IPSec Wizard Step 2 of 3: Remote Information Remote Identifier <input type="text"/> <input type="button" value="Back"/> <input type="button" value="Next"/>
Quick Start	
Configuration	
LAN	
WAN	
System	
Firewall	
VPN	
IPSec	
IPSec Wizard	
IPSec Policy	
PPTP	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

Remote Identifier: The Identifier of remote gateway, all input value type will be auto-defined as IP Address, FQDN(DNS) or FQUN(E-mail).

Back: Back to the Previous page.

Next: Go to the next page.

(5)LAN to Host (For BiGuard VPN Client only): BiGuard would like to establish an IPSec VPN tunnel with BiGuard VPN Client software C01 by using aggressive mode.

Status	<h3>IPSec Wizard</h3> <p>Step 2 of 3: Remote Information</p> <p>VPN Client IP Address <input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="100"/> <input type="text" value="1"/></p> <p> 1. Please note that this field must be consistent with the setting of VPN Client. 2. Be sure that each client must use different VPN Client IP Address.</p> <p><input type="button" value="Back"/> <input type="button" value="Next"/></p>
Quick Start	
Configuration	
LAN	
WAN	
System	
Firewall	
VPN	
IPSec	
IPSec Wizard	
IPSec Policy	
PPTP	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

VPN Client IP Address: The VPN Client Address for BiGuard VPN Client, this value will be apply on both **remote ID** and remote **Network** as single address.

Back: Back to the Previous page.

Next: Go to the next page.

<h3>IPSec Wizard</h3>				
Configuration Summary				
Connection Name		Tunnel		
Tunnel		Enabled		
Local	ID	WAN IP Address	Type	IP Address
	Network	192.168.1.254/255.255.255.0	Type	Subnet
Remote	Secure Gateway	200.200.200.1	Type	IP Address/ Hostname
	ID	Remote Secure Gateway IP Address	Type	IP Address
	Network	192.168.3.0/255.255.255.0	Type	Subnet
Proposal	Secure Association	Main Mode		
	Method	ESP		
	Encryption Protocol	3DES		
	Authentication Protocol	MD5		
	Perfect Forward Secure	Enabled		
	Key Group	Group 2		
	PreShared Key	12345678		
	IKE Life Time	3600 seconds		
Key Life Time	28800 seconds			
<input type="button" value="Back"/>		<input type="button" value="Done"/>		

After your configuration is done, you will see a **Configuration Summary**.

Back: Back to the Previous page.

Done: Click **Done** to apply the rule.

4.4.5.1.2 IPSec Policy

IPSec					
IPSec Tunnels					
Name	Enable	Local Network	Remote Network	Remote Gateway	IPSec Proposal
Create					

Click **Create** to create a new IPSec VPN connection account.

Configuring a New VPN Connection

IPSec			
Create			
Connection Name	<input type="text"/>		
Tunnel	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Local			
ID	<input type="text" value="IP Address"/> ▾	Data	<input type="text"/>
Network	<input type="text" value="Any Local Address"/> ▾	IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		End IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		Netmask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Remote			
Secure Gateway	<input type="text" value="IP Address/ Hostname"/> ▾	Data	<input type="text"/>
ID	<input type="text" value="IP Address"/> ▾	Data	<input type="text"/>
Network	<input type="text" value="Subnet"/> ▾	IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		End IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		Netmask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Proposal			
Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key		
Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Protocol	<input type="text" value="3DES"/> ▾		
Authentication Protocol	<input type="text" value="MD5"/> ▾		
Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
PreShared Key	<input type="text"/>		
IKE Life Time	<input type="text" value="28800"/>	Seconds	
Key Life Time	<input type="text" value="3600"/>	Seconds	
Netbios Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
DPD Setting			
DPD Function	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
Detection Interval	<input type="text" value="30"/>	seconds	
Idle Timeout	<input type="text" value="4"/>	consecutive times	
<input type="button" value="Apply"/>			

Connection Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate this tunnel. Select **Disable** to deactivate this tunnel.

Local: This section configures the local host.

ID: This is the identity type of the local router or host. Choose from the following four options:

WAN IP Address: Automatically use the current WAN Address as ID

IP Address: Use an IP address format.

FQDN DNS(Fully Qualified Domain Name): Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name,

VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.

FQUN E-Mail(Fully Qualified User Name): Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.

Data: Enter the ID data using the specific ID type.

Network: Set the IP address, IP range, subnet, or address range of the local network.

Any Local Address: Will enable any local address on the network.

Subnet: The subnet of the local network. Selecting this option enables you to enter an IP address and netmask.

IP Range: The IP Range of the Local network.

Single Address: The IP address of the local host.

Remote: This section configures the remote host.

Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

ID: The identity type of the local host. Choose from the following three options:

Remote IP Address: Automatically use the remote gateway Address as ID with ID type – IP Address.

IP Address: Use an IP address format.

FQDN DNS(Fully Qualified Domain Name): Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name, VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.

FQUN E-Mail(Fully Qualified User Name): Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.

Data: Enter the ID data using the specific ID type.

Network: Set the subnet, IP Range, single address, or gateway address of the remote network.

Subnet: The subnet of the remote network. Selecting this option allows you to enter an IP address and netmask.

IP Range: The IP Range of the remote network.

Single Address: The IP address of the remote host.

Gateway Address: The gateway address of the remote host.

Proposal:

Secure Association (SA): SA is a method of establishing a security policy between two points. There are three methods of creating SA, each varying in

degrees of security and speed of negotiation:

Main Mode: Uses the automated Internet Key Exchange (IKE) setup; most secure method with the highest level of security.

Aggressive Mode: Uses the automated Internet Key Exchange (IKE) setup; mid-level security. Speed is faster than Main mode.

Manual Key: Standard level of security. It is the fastest of the three methods.

Method: There are two methods of checking the authentication information, AH (Authentication Header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. AH data will be authenticated but not encrypted.

Encryption Protocol: Select the encryption method from the pull-down menu. There are several options: DES, 3DES, and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

DES: Stands for Data Encryption Standard. It uses a 56-bit encryption method.

3DES: Stands for Triple Data Encryption Standard. It uses a 168-bit encryption method.

AES: Stands for Advanced Encryption Standard. You can use 128, 192 or 256 bits as encryption method.

Authentication Protocol: Authentication establishes data integrity and ensures it is not tampered with while in transit. There are two options: Message Digest 5 (MD5), and Secure Hash Algorithm (SHA1). While slower, SHA1 is more resistant to brute-force attacks than MD5.

MD5: A one-way hashing algorithm that produces a 128-bit hash.

SHA1: A one-way hashing algorithm that produces a 160-bit hash.

Perfect Forward Secure: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over the Internet.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

IKE Life Time: Allows you to specify the timer interval for renegotiation of the IKE security association. The value is in seconds, e.g. 28800 seconds = 8 hours.

Key Life Time: Allows you to specify the timer interval for renegotiation of another key. The value is in seconds e.g. 3600 seconds = 1 hour.

Netbios Broadcast: Allows BiGuard to send local Netbios Broadcast packet through the IPSec Tunnel, please select **Enable** or **Disable**.

DPD Setting: DPD, Dead Peer Detection.

DPD Function: Select Enable or Disable DPD function.

Detection Interval: please input the interval time to send out DPD packet.

Idle Timeout: Please input the consecutive no response time to disconnect this tunnel.

Click the **Apply** button to save your changes.

After you have created the IPSec connection, the account information will be displayed:

IPSec							
IPSec Tunnels							
Name	Enable	Local Network	Remote Network	Remote Gateway	IPSec Proposal		
Tunnel	✓	Any	Any	200.200.200.1	MAIN Mode ESP [3DES: MD5]	Edit ▶	Delete ▶
Create ▶							

Name: This is the user-defined name of the connection.

Enable: This function activates or deactivates the IPSec connection.

Local Subnet: Displays IP address and subnet of the local network.

Remote Subnet: Displays IP address and subnet of the remote network.

Remote Gateway: This is the IP address or Domain Name of the remote VPN device that is connected and has an established IPSec tunnel.

IPSec Proposal: This is the selected IPSec security method.

For examples on how to apply IPSec to your network, see **Appendix F: IPSec Logs and Events**.


4.4.5.2 PPTP

PPTP is a set of protocols that enable Virtual Private Networks (VPN). VPN is a way to establish secured communication tunnels to an organization's network via the Internet.

PPTP

General Setting

PPTP function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Auth. Type	Pap or Chap ▾
Data Encryption	Enable ▾
Encryption Key Length	Auto ▾
Peer Encryption Mode	Only Stateless ▾
IP Addresses Assigned to Peer	Start from: 192.168.1.200
Idle Timeout	0 Min.

( Enable data encryption will use MS-CHAPv2 to authenticate the peer.)

Account Setting

Name	Enable	Type	Peer Network
Create ▶			

PPTP function: Select **Enable** to activate PPTP Server. **Disable** to deactivate PPTP Server function.

Auth. Type: The authentication type, **Pap or Chap, PaP, Chap**.

Data Encryption: Select **Enable** or **Disable** the Data Encryption.

Encryption Key Length: **Auto, 40 bits** or **128 bits**.

Peer Encryption Mode: **Only Stateless** or **Allow Stateless and Stateful**.

IP Addresses Assigned to Peer Start from: 192.168.1.x: please input the IP assigned range from **1 ~ 254** (except BiGuard 30's LAN IP address with **192.168.1.254** as BiGuard 30's default LAN IP address and IP pool range of DHCP server settings with **100~199** as BiGuard 30's default DHCP IP pool range.)

Idle Timeout " " Min: Specify the time for remote peer to be disconnected without any activities, from **0~120**.

Click **Create** to create a new PPTP VPN connection account.

Status	
Quick Start	
Configuration	
LAN	
WAN	
System	
Firewall	
VPN	
IPSec	
PPTP	
QoS	
Virtual Server	
Advanced	
Save Config to Flash	

PPTP	
Add PPTP Account	
Connection Name	<input type="text"/>
Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Retype Password	<input type="text"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN
Peer Network IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Peer Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Netbios Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/>	

Connection Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate this tunnel. Select **Disable** to deactivate this tunnel.

Username: Please input the username for this account.

Password: Please input the password for this account.

Retype Password: Please repeat the same password as previous field.

Connection Type: Select **Remote Access** for single user, Select **LAN to LAN** for remote gateway.

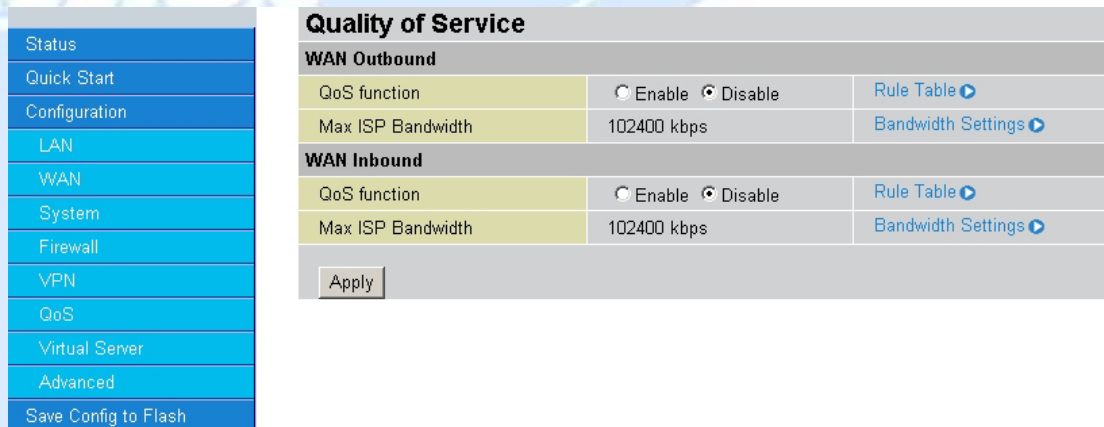
Peer Network IP: Please input the IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

Netbios Broadcast: Allows BiGuard to send local Netbios Broadcast packet through the PPTP Tunnel, please select **Enable** or **Disable**.

4.4.6 QoS

BiGuard 2/10 can optimize your bandwidth by assigning priority to both inbound and outbound data with QoS. This menu allows you to configure QoS for both inbound and outbound traffic.



The first menu screen gives you an overview of which WAN ports currently have QoS active, and the bandwidth settings for each.

WAN Outbound:

QoS Function: QoS status for WAN outbound. Select **Enable** to activate QoS for WAN's outgoing traffic. Select **Disable** to deactivate.

Max ISP Bandwidth: The maximum bandwidth afforded by the ISP for WAN's outbound traffic.

WAN Inbound:

QoS Function: QoS status for WAN inbound. Select **Enable** to activate QoS for WAN's incoming traffic. Select **Disable** to deactivate.

Max ISP Bandwidth: The maximum bandwidth afforded by the ISP for WAN's inbound traffic.

Creating a New QoS Rule

To get started using QoS, you will need to establish QoS rules. These rules tell the BiGuard 2/10 how to handle both incoming and outgoing traffic. The following example shows you how to configure WAN Outbound QoS. Configuring the other traffic types follows the same process.

To make a new rule, click **Rule Table**. This will bring you to the Rule Table which displays the rules currently in effect.

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Quality of Service					
WAN Outbound QoS Rule Table (total 0 rules used / maximum 40 rules.)					
Application	Guaranteed	Maximum	Priority		
Non-Assigned Bandwidth Ratio		100% (102400 kbps)			
Create					

Next, click **Create** to open the QoS Rule Configuration window.

- Status
- Quick Start
- Configuration
- LAN
- WAN
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

Quality of Service			
Add QoS Rule			
Interface	WAN Outbound		
Application	<input type="text"/>		
Guaranteed	<input type="text" value="1"/>	%	
Maximum	<input type="text" value="100"/>	%	
Priority	3 (Normal)		
DSCP Marking	Disable		
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address		
Bandwidth Type	<input checked="" type="radio"/> Shared Bandwidth <input type="radio"/> Bandwidth per Source IP Address		
Source IP Address Range	From <input type="text" value="0.0.0.0"/>	To	<input type="text" value="255.255.255.255"/>
Destination IP Address Range	From <input type="text" value="0.0.0.0"/>	To	<input type="text" value="255.255.255.255"/>
Protocol	Any		
Source Port Range Helper	From <input type="text" value="1"/>	To	<input type="text" value="65535"/>
Destination Port Range Helper	From <input type="text" value="1"/>	To	<input type="text" value="65535"/>
Apply			

- Application: User defined application name for the current rule.
- Packet Type: The type of packet this rule applies to. Choose from **Any**, **TCP**, **UDP**, or **ICMP**.
- Guaranteed: The guaranteed amount of bandwidth for this rule as a percentage.
- Maximum: The maximum amount of bandwidth for this rule as a percentage.
- Priority: The priority assigned to this service. Select a value from 0 to 6, 0 being highest.
- DSCP Marking: Used to classify traffic. Select from **Best Effort**, **Premium**, **Gold Service (High Medium, Low)**, **Silver (H,M,L)**, and **Bronze (H,M,L)**.
- Address Type: The type of address this rule applies to. Select **IP Address** or **MAC Address**.
- Bandwidth Type:
 - Shared Bandwidth: Please select **Shared Bandwidth** if you would like the specified bandwidth to be shared for all IP address in specified IP range.

Bandwidth per source IP Address: Please select **Bandwidth per source IP Address** if you would like the specified bandwidth to be applied individually per source IP address in specified IP range.

For IP Address (default)...

Source IP Address Range: The range of source IP Addresses this rule applies to.

Destination IP Address Range: The range of destination IP Addresses this rule applies to.

Source Port Range: The range of source ports this rule applies to.

Destination Port Range: The range of destination ports this rule applies to.

Helper: You could also select the application type you would like to apply for automatic input.

Click **Apply** to save your changes.

For MAC Address:

Status	Quality of Service	
Quick Start	Add QoS Rule	
Configuration	Interface	WAN Outbound
LAN	Application	<input type="text"/>
WAN	Guaranteed	<input type="text" value="1"/> %
System	Maximum	<input type="text" value="100"/> %
Firewall	Priority	<input type="text" value="3 (Normal)"/>
VPN	DSCP Marking	<input type="text" value="Disable"/>
QoS	Address Type	<input type="radio"/> IP Address <input checked="" type="radio"/> MAC Address
Virtual Server	Source MAC Address Candidates	<input type="text"/> (ex. xx:xx:xx:xx:xx:xx)
Advanced	Protocol	<input type="text" value="Any"/>
Save Config to Flash	Source Port Range Helper	From <input type="text" value="1"/> To <input type="text" value="65535"/>
	Destination Port Range Helper	From <input type="text" value="1"/> To <input type="text" value="65535"/>
	<input type="button" value="Apply"/>	

Source MAC Address: The source MAC Address of the device this rule applies to.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

Source Port Range: The range of source ports this rule applies to.

Destination Port Range: The range of destination ports this rule applies to.

Click **Apply** to save your changes.

Helper: You could also select the application type you would like to apply for automatic input.

4.4.7 Virtual Server

In TCP/IP and UDP networks, a port is a 16-bit number used to identify which

application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the Internet Assigned Numbers Authority (IANA), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

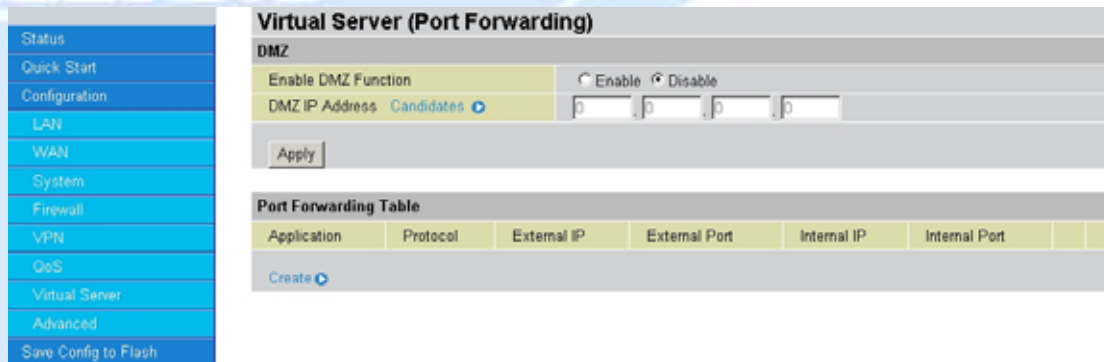
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. peer-to-peer applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server. The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN Configuration** section of this manual for more information on NAT.

BiGuard 2/10 can also be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

4.4.7.1 DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

Caution: Such Local computer exposure to the Internet may face a variety of security risks.



Enable DMZ function:

Enable: Activates your router's DMZ function.

Disable: Default setting. Disables the DMZ function.

DMZ IP Address: Give a static IP address to the DMZ Host when the **Enable** radio button is selected. Be aware this IP will be exposed to the WAN/Internet.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

Select the **Apply** button to apply your changes.

4.4.7.2 Port Forwarding

Because NAT can act as a "natural" Internet firewall, your router protects your network from being accessed by outside users, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a "virtual server". You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request is received, it will be forwarded to the corresponding internal server.

Click **Create** to add a new port forwarding rule. There are two port forwarding modes: **Port Range Mapping** and **Port Redirection**.

This function allows any incoming data addressed to a range of service port numbers (from the Internet/WAN Port) to be re-directed to a particular LAN private/internal IP address. This option gives you the ability to handle applications that use more than one port such as games and audio/video conferencing.

Application: User defined application name for the current rule.

Helper: You could also select the application type you would like to apply for automatic input.

Protocol type: please select protocol type

External Port: Enter the port number of the service that will be sent to the Internal IP address.

Redirect Port: Enter a new port number for the service that will be sent to the Internal IP address.

External Port Range: Enter the port number of the service that will be sent to the Internal IP address.

External IP Address: Please click candidate to select the WAN interface or the WAN IP address.

Internal IP Address: Enter the LAN server/host IP address that the service request from the Internet will be sent to.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

NOTE: You need to give your LAN server/host a static IP address for the Virtual Server to work properly.

Click **Apply** to save your changes.

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason, using specific Virtual Server entries just for the ports your application requires, instead of using DMZ is recommended.

4.4.8 Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of BiGuard 2/10. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

There are five items within the Advanced section: Static Route, Dynamic DNS ,Device Management, IGMP and VLAN Bridge.

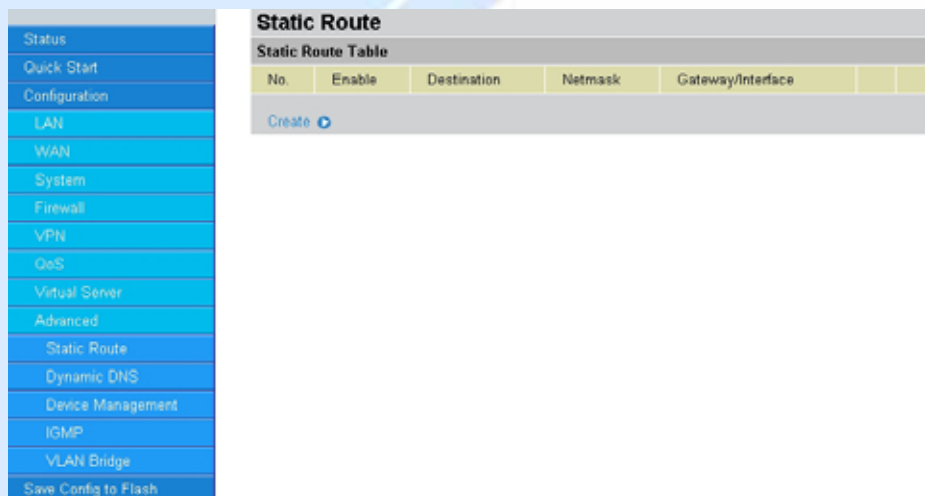
Advanced
Static Route
Dynamic DNS
Device Management
IGMP
VLAN Bridge

There are three items within the Advanced section: Static Route, Dynamic DNS and Device Management.

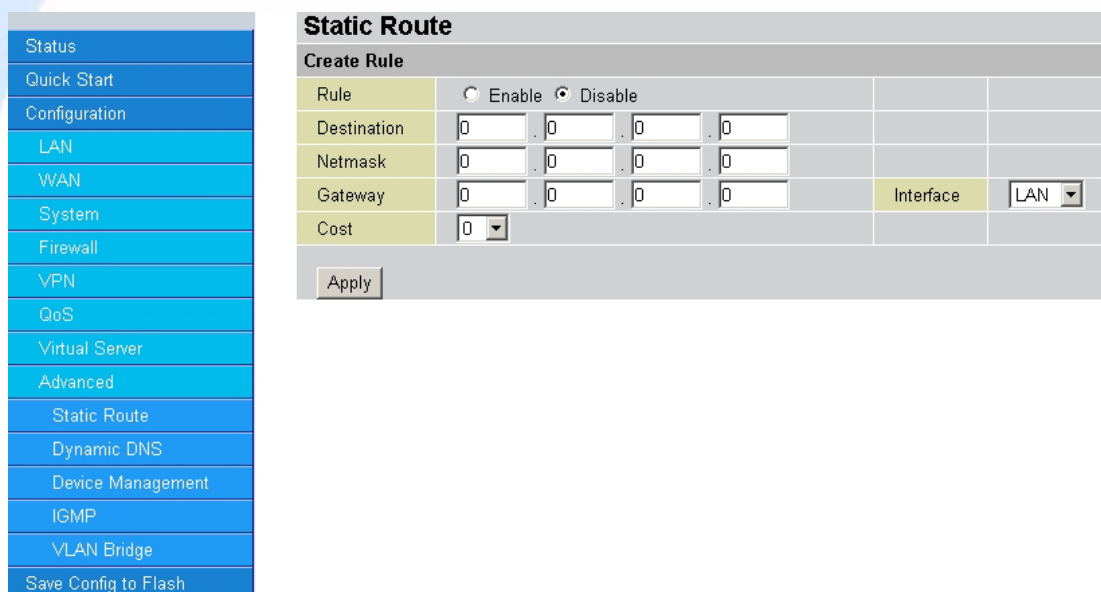
4.4.8.1 Static Route

The static route settings enable the router to route IP packets to another network

(subnet). The routing table stores the routing information so the router knows where to redirect the IP packets.



Click on **Static Route** and then click **Create** to add a routing table.



Rule: Select Enable to activate this rule, Disable to deactivate this rule.

Destination: This is the destination subnet IP address.

Netmask: This is the subnet mask of the destination IP addresses based on above destination subnet IP.

Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop.

Click **Apply** to save your changes.

4.4.8.2 Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful when hosting servers via your WAN connection, so that anyone wishing to connect to you may use your domain name, rather than having to use a dynamic IP address that changes periodically. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP. Click **Edit** in the Dynamic DNS Settings Table to set related parameters for a specific interface.

Status	Dynamic DNS Settings	
Quick Start	Parameters	
Configuration	Dynamic DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN	Dynamic DNS Server	NONE
WAN	Wildcard	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
System	Domain Name	
Firewall	Username	
VPN	Password	
QoS	<input type="button" value="Apply"/>	
Virtual Server		
Advanced		
Static Route		
Dynamic DNS		
Device Management		
IGMP		
VLAN Bridge		
Save Config to Flash		

You will first need to register and establish an account with the Dynamic DNS provider using their website,

Example: DYNDNS

<http://www.dyndns.org/>

(BiGuard 2/10 supports several Dynamic DNS providers , such as

www.zoneedit.com , www.orgdns.org , www.dhs.org , www.dyns.cx ,
www.3domain.hk , www.dyndns.org , www.3322.org)

Dynamic DNS:

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The following fields will be activated and required:

Dynamic DNS Server: Select the DDNS service you have established an account with.

Wildcard: Select this check box to enable the DYNDNS Wildcard.

Domain Name: Enter your registered domain name for this service.

Username: Enter your registered user name for this service.

Password: Enter your registered password for this service.

Click **Apply** to save your changes.

4.4.8.3 Device Management

The Device Management Advanced Configuration settings allow you to control your router's security options and device monitoring features.

Device Management			
Device Name			
Name	BiGuard10		
Web Server Settings			
* HTTP Port	80	(80 is default HTTP port)	
Management IP Address	0 . 0 . 0 . 0	(0.0.0.0 means Any)	
Expire to auto-logout	300	seconds	
SNMP Access Control			
SNMP Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write		
*: This setting will become effective after you save to flash and restart the router.			
Apply			

SAVE CONFIG RESTART LOGOUT

Device Name

Name: Enter a name for this device.

Web Server Settings

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

Example: User A changes HTTP port number to 100, specifies their own IP address of 192.168.1.100 and sets the logout time to be 100 seconds. The router will only allow User A access from the IP address 192.168.1.100 to logon to the Web GUI by typing: `http://192.168.1.254:100` in their web browser. After 100 seconds, the device will automatically logout User A.

SNMP Access Control

SNMP Function: Select **Enable** to activate this function, **Disable** to deactivate this function.

SNMP V1 and V2

Read Community: Input the string for Read community to match your SNMP software.

Write Community: Input the string for Write community to match your SNMP software.

Trap Community: Input the string for Trap community to match your SNMP software.

IP Address: Input the device IP address with SNMP software installed.

SNMP V3

Username: Input the Username for your SNMP software.

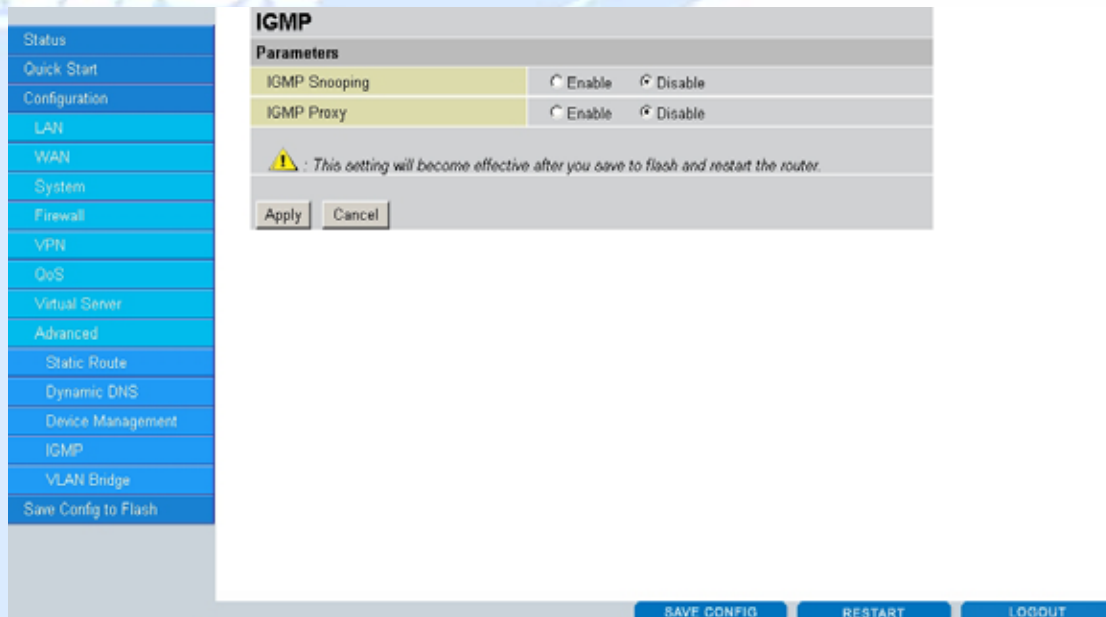
Password: Input the Password for your SNMP software.

Access Right: Select Read to allow your SNMP software to read the information.

Select Read/Write to allow your SNMP software to read and write the information.

4.4.8.4 IGMP

IGMP snooping and IGMP proxy are functions to be used for home users who will access IPTV applications.



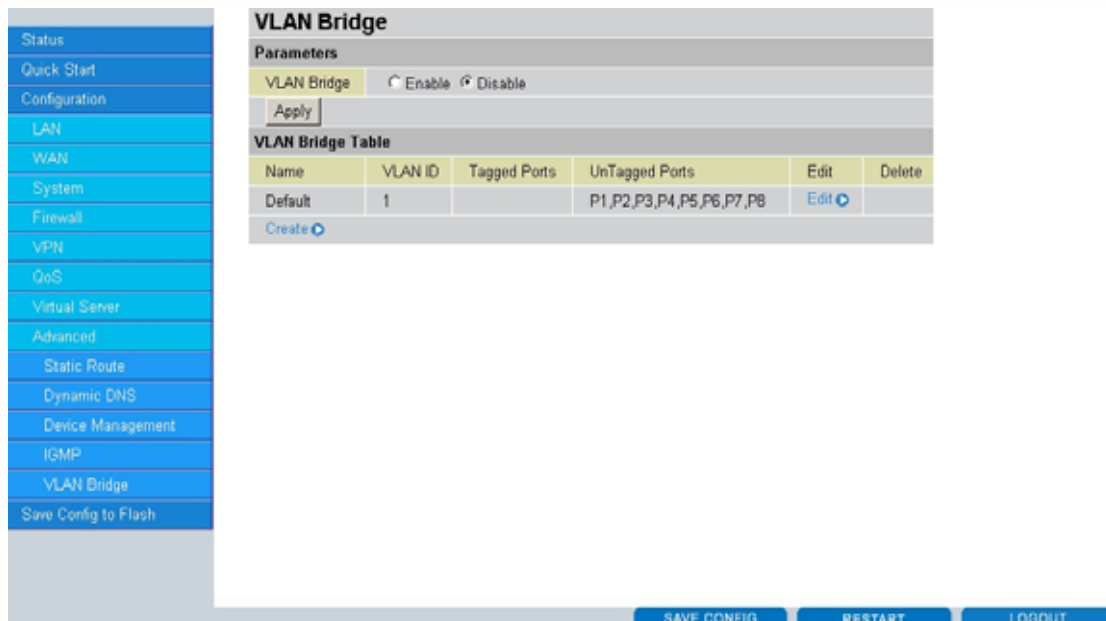
IGMP Snooping: Please select enable or disable IGMP Snooping function.

IGMP Proxy: Please select enable or disable the IGMP Proxy function.

Click Apply to apply this function, and please note that the setting will become effective after you save to flash and restart the router.

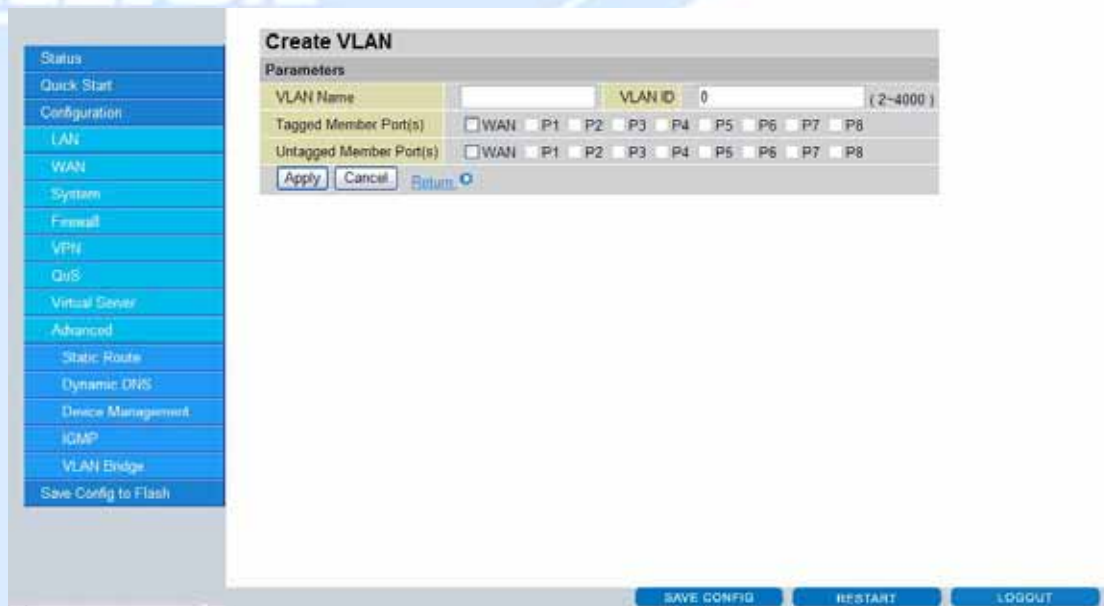
4.4.8.5 VLAN Bridge

This section allows you to create VLAN group and specify the member.



VLAN Bridge: Select enable or disable to use VLAN Bridge function.

Click Create to create another VLAN group.



VLAN Name: Please input VLAN name of this rule.

VLAN ID: Please input VLAN ID that will be used for Tagged member port(s).

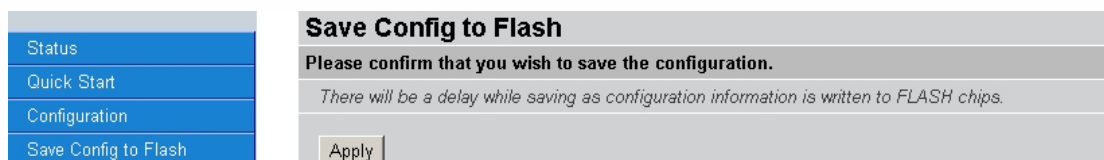
Tagged Member port(s): Please check the interface that you would like to use in this VLAN ID group.

Untagged Member port(s): Please check the interface that you would like to use in this VLAN ID group.

Click Apply to add this rule.

4.5 Save Configuration To Flash

After changing the router's configuration settings, you must save all of the configuration parameters to flash memory to avoid them being lost after turning off or resetting your router. Click **Apply** to write your new configuration to flash memory.



4.6 Logout

To exit the router's web interface, click **Logout**. Please ensure that you have saved

your configuration settings before you logout.



Be aware that the router is restricted to only one PC accessing the web configuration interface at a time. Once a PC has logged into the web interface, other PCs cannot gain access until the current PC has logged out. If the previous PC forgets to logout, the second PC can access the page after a user-defined period (5 minutes by default). You can modify this value using the **Advanced > Device Management** section of the Web Configuration Interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

5.1 Basic Functionality

This section deals with issues regarding your BiGuard 2/10's basic functions.

5.1.1 Router Won't Turn On

If the Power and other LEDs fail to light when your BiGuard 2/10 is turned on:

- Make sure that the power cord is properly connected to your firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by Billion for this product.

If the error persists, you may have a hardware problem, and should contact technical support.

5.1.2 LEDs Never Turn Off

When your BiGuard 2/10 is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there may be a hardware problem.

If all LEDs are still on one minute after powering up:

- Cycle the power to see if the router recovers.
- Clear the configuration to factory defaults.

If the error persists, you may have a hardware problem, and should contact technical support.

5.1.3 LAN or Internet Port Not On

If either the LAN LEDs or Internet LED does not light when the Ethernet connection is made, check the following:

- Make sure each Ethernet cable connection is secure at the firewall and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable. When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

5.1.4 Forgot My Password

Try entering the default User Name and Password:

User Name: admin

Password: admin

Please note that both the User Name and Password are case-sensitive.

If this fails, you can restore your BiGuard 2/10 to its factory default settings by holding the Reset button on the back of your router until the Status LED begins to blink. Then enter the default User Name and Password to access your router.

5.2 LAN Interface

Refer to this section for issues relating to BiGuard 2/10's LAN Interface.

5.2.1 Can't Access BiGuard 2/10 from the LAN

If there is no response from BiGuard 2/10 from the LAN:

- Check your Ethernet cable types and each connection.
- Make sure the computer's Ethernet adapter is installed and functioning properly.

If the error persists, you may have a hardware problem, and should contact technical support.

5.2.2 Can't Ping Any PC on the LAN

If PCs connected to the LAN cannot be pinged:

- Check the 10/100 LAN LEDs on BiGuard 2/10's front panel. One of these LEDs should be on. If they are both off, check the cables between BiGuard 2/10 and the hub or PC.
- Check the corresponding LAN LEDs on your PC's Ethernet device are on.
- Make sure that driver software for your PC's Ethernet adapter and TCP/IP software is correctly installed and configured on your PC.
- Verify the IP address and the subnet mask of BiGuard 2/10 and the computers are on the same subnet.

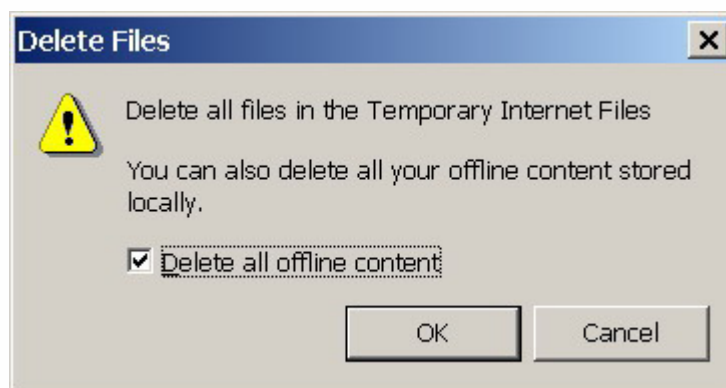
5.2.3 Can't Access Web Configuration Interface

If you are having trouble accessing BiGuard 2/10's Web Configuration Interface from a PC connected to the network:

- Check the connection between the PC and the router.
- Make sure your PC's IP address is on the same subnet as the router.
- If your BiGuard 2/10's IP address has changed and you don't know the current IP address, reset the router to factory defaults by holding the Reset button on the back of your router for 6 seconds. This will reset the router's IP address to 192.168.1.254.
- Check to see if your browser had Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to ensure that the Java applet is loaded.
- Try closing the browser and re-launching it.
- Make sure you are using the correct **User Name and Password**. User Names and Passwords are case-sensitive, so make sure that **CAPS LOCK** is not on when entering this information.
- Try clearing your browser's cache.
 1. With Internet Explorer, click **Tools > Internet Options**.
 2. Under the **General** tab, click **Delete Files**.



3. Make sure that the **Delete All Offline Content** checkbox is checked, and click **OK**.



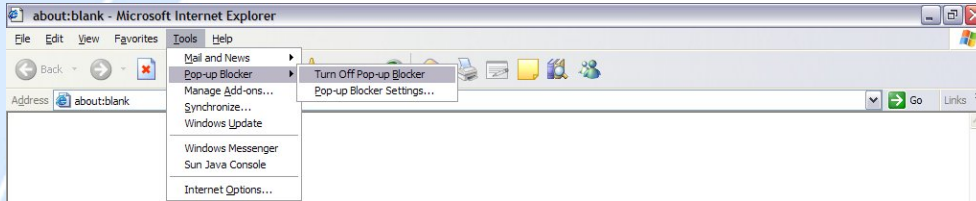
4. Click **OK** under **Internet Options** to close the dialogue.
- In Windows, type **arp -d** at the command prompt to clear you computer's ARP table.

5.2.3.1 Pop-up Windows

To use the Web Configuration Interface, you need to disable pop-up blocking. You can either disable pop-up blocking, which is enabled by default in Windows XP Service Pack 2, or create an exception for your BiGuard 2/10's IP address.

Disabling All Pop-ups

In Internet Explorer, select **Tools > Pop-up Blocker** and select **Turn Off Pop-up Blocker**.



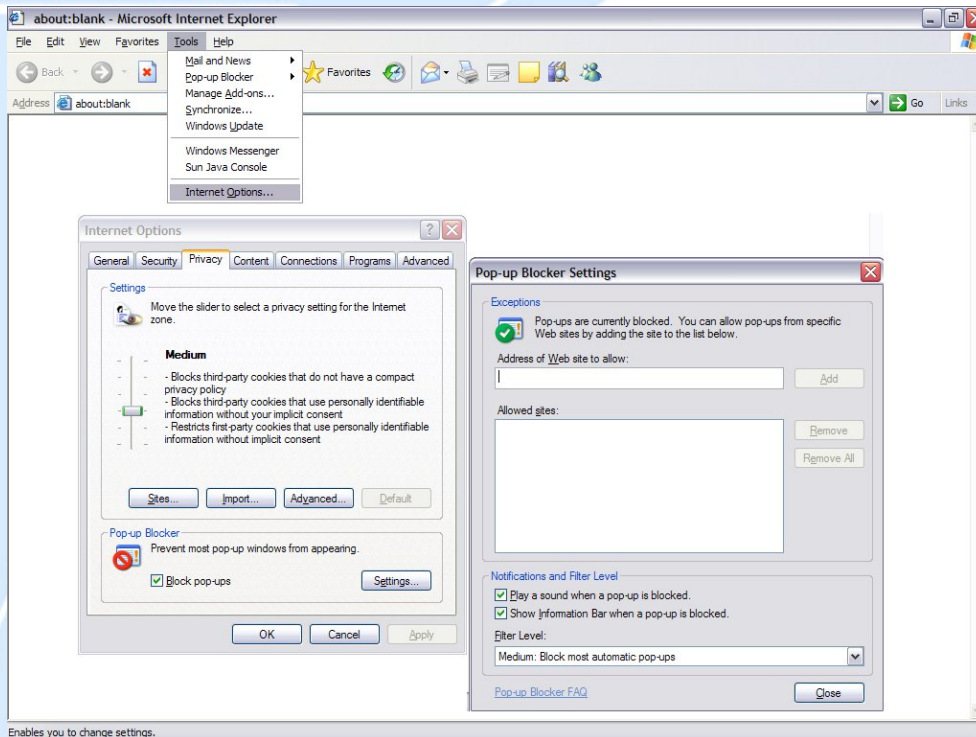
You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab of the **Internet Options** dialogue.

1. In Internet Explorer, select **Tools > Internet Options**.
2. Under the **Privacy** tab, clear the **Block pop-ups** checkbox and click **Apply** to save your changes.

Enabling Pop-up Blockers with Exceptions

If you only want to allow pop-up windows with your BiGuard 2/10:

1. In Internet Explorer, select **Tools > Internet Options**.
2. Under the **Privacy** tab, click **Settings** to open the **Pop-up Blocker Settings** dialogue.

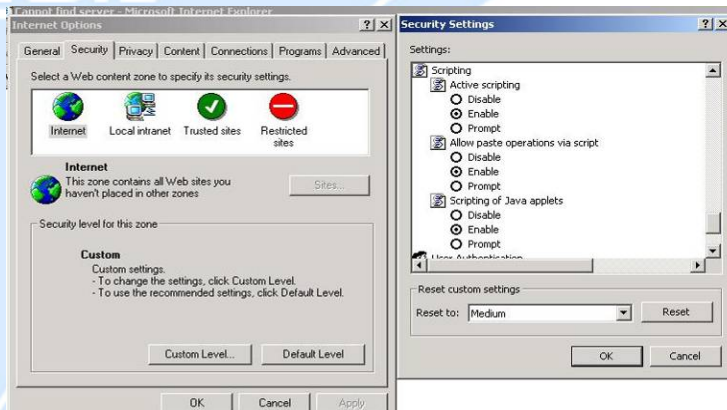


3. Enter the IP address of your router.
4. Click **Add** to add the IP address to the list of **Allowed sites**.
5. Click **Close** to return to the **Privacy** tab of the **Internet Options** dialogue.
6. Click **Apply** to save your changes.

5.2.3.2 Javascripts

If the Web Configuration Interface is not displaying properly in your browser, check to make sure that JavaScripts are allowed.

1. In Internet Explorer, click **Tools > Internet Options**.
2. Under the **Security** tab, click **Custom Level**.

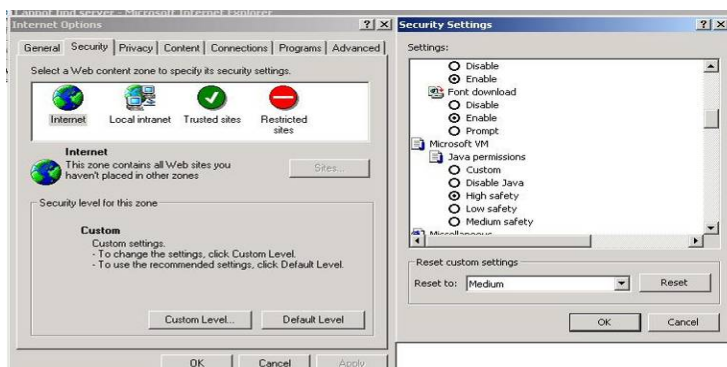


3. Under **Scripting**, check to see if **Active scripting** is set to **Enable**.
4. Ensure that **Scripting of Java applets** is set to **Enable**.
5. Click **OK** to close the dialogue.

5.2.3.3 Java Permissions

The following Java Permissions should also be given for the Web Configuration Interface to display properly:

1. In Internet Explorer, click **Tools > Internet Options**.
2. Under the **Security** tab, click **Custom Level**.



3. Under **Microsoft VM***, make sure that a safety level for **Java permissions** is selected.
4. Click **OK** to close the dialogue.

NOTE: If Java from Sun Microsystems is installed, scroll down to **Java (Sun)** and ensure that the checkbox is filled.

5.3 WAN Interface

If you are having problems with the WAN Interface, refer to the tips below.

5.3.1 Can't Get WAN IP Address from the ISP

If the WAN IP address cannot be obtained from the ISP:

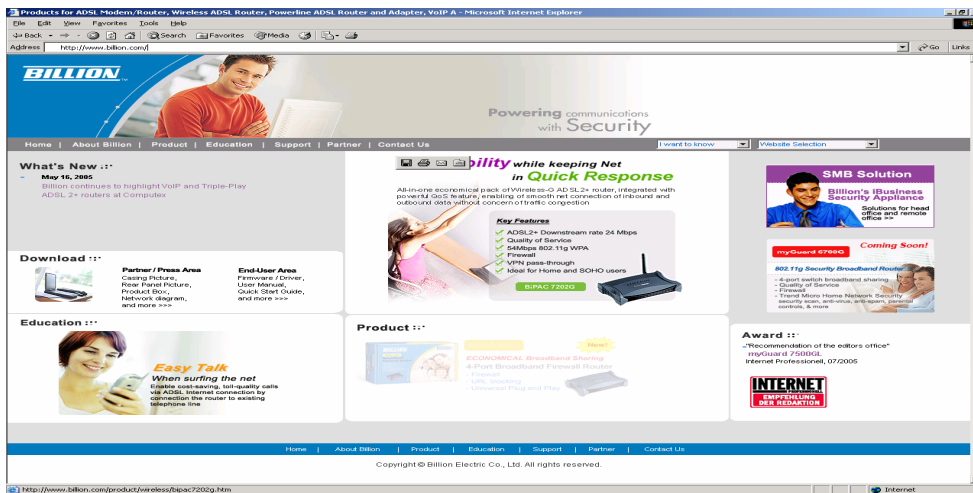
- If you are using PPPoE or PPTP, you will need a user name and password. Ensure that you have entered the correct **Service Type, User Name, and Password**. Note that user names and passwords are case-sensitive.
- If your ISP requires MAC address authentication, clone the MAC address from your PC on the LAN as BiGuard 2/10's WAN MAC address.
- If your ISP requires host name authentication, configure your PC's name as BiGuard 2/10's system name.

5.4 ISP Connection

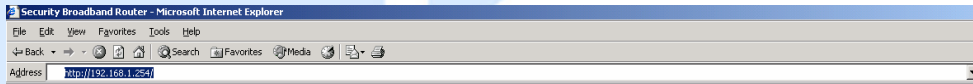
Unless you have been assigned a static IP address by your ISP, your BiGuard 2/10 will need to request an IP address from the ISP in order to access the Internet. If your BiGuard 2/10 is unable to access the Internet, first determine if your router is able to obtain a WAN IP address from the ISP.

To check the WAN IP address:

1. Open your browser and choose an external site (i.e. www.billion.com).



2. Access the Web Configuration Interface by entering your router's IP address (default is 192.168.1.254).



3. The WAN IP Status is displayed on the first page.



BiGuard 2 iBusiness Security Gateway Home-Office

Powering communications with Security

Status Refresh

Device Information

Device Name	BiGuard2
Private LAN Mac Address	00:13:31:45:26:FF
Public WAN Mac Address	00:13:31:45:27:00
Firmware Version	1.01
Home URL	Billion Electric Co., Ltd.

LAN

IP Address	192.168.1.254
Netmask	255.255.255.0
DHCP Server	Enabled

WAN

Connection Method	Connect by Static IP Settings
IP Address	211.21.69.53
Netmask	255.255.255.248
Gateway	211.21.69.49
DNS	168.95.192.1 168.95.1.1

4. Check to see that the WAN port is properly connected to the ISP. If a **Connected by (x)** where **(x)** is your connection method is not shown, your router has not successfully obtained an IP address from your ISP.

If an IP address cannot be obtained:

1. Turn off the power to your cable or DSL modem.
2. Turn off the power to your BiGuard 2/10.
3. Wait five minutes and power on your cable or DSL modem.
4. When the modem has finished synchronizing with the ISP (generally shown by LEDs on the modem), turn on the power to your router.

If an IP address still cannot be obtained:

- Your ISP may require a login program. Consult your ISP whether they require PPPoE or some other type of login.
- If your ISP requires a login, check to see that your User Name and Password are entered correctly.
- Your ISP may check for your PC's host name. Assign the PC Host Name of your ISP

account as your PC's host name on the router.

- Your ISP may check for your PCs MAC address. Either inform your ISP that you have purchased a new network device and ask them to use your router's MAC address, or configure your router to spoof your PC's MAC address.

If an IP address can be obtained, but your PC cannot load any web pages from the Internet:

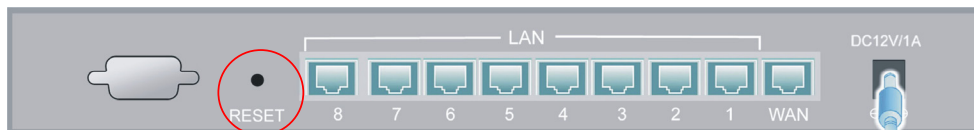
- Your PC may not recognize DNS server addresses. Configure your PC manually with DNS addresses.
- Your PC may not have the router correctly configured as its TCP/IP gateway.

5.5 Problems with Date and Time

If the date and time is not being displayed correctly, be sure to set it for your BiGuard 2/10 via the Web Configuration Interface. Both date and time can be found under **Configuration > System > Time Zone**.

5.6 Restoring Factory Defaults

You can restore your BiGuard 2/10 to its factory settings by holding the Reset button on the back of your router until the Status LED begins to blink. This will reset your router to its default settings.



Appendix A: Product Specifications

A.1 BiGuard 10 Product Specifications



Virtual Private Network

- IPsec VPN, supports up to 10 IPsec tunnels
- IPsec VPN performance is up to 20 Mbps
- PPTP VPN, support up to 4 PPTP tunnels
- PPTP VPN performance is up to 10 Mbps
- Manual key, Internet Key Exchange (IKE) authentication and Key Management
- Authentication (MD5 / SHA-1)
- DES/3DES encryption
- AES 128/192/256 encryption
- IP Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)
- IPsec VPN concentrator
- Dynamic IPsec VPN (FQDN) support
- IPsec NAT Traversal (IPsec NAT-T)
- IPsec DPD (Dead Peer Detection)
- Supports remote access and office-to-office IPsec Connections
- PPTP Server
- Netbios over VPN

Firewall

- Stateful Packet Inspection (SPI) and Denial of Service (DoS) prevention
- Packet filter un-permitted inbound (WAN)/Inbound (LAN) Internet access by IP address, port number and packet type
- Email alert and logs of attack
- MAC Address Filtering

- Intrusion detection

Content Filtering

- URL Filter settings prevent user access to certain sites on the Internet
- Java Applet/Active X/Cookie Blocking

Quality of Service Control

- Supports DiffServ approach
- Traffic prioritization and bandwidth management based-on IP protocol, port number and IP or MAC address

Web-Based Management

- Easy-to-use WEB interface
- Firmware upgradeable via WEB interface
- Local and remote management via HTTP & HTTPS

Network Protocols and Features

- Web Diagnostics
- System Logs
- PPPoE, PPTP, Big Pond and DHCP client connections to the ISP
- NAT, static routing and RIP-2
- Router Mode (NAT Disable)
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- DHCP Server
- NTP
- SMTP Client
- SNMP
- SIP Pass-through
- IGMP snooping & IGMP Proxy
- Port based VLAN Bridge mode
- Multiple NAT (Multiple LAN & Multiple WAN)

Physical Interface

Ethernet WAN 1 ports (10/100 Base-T), support Auto- Crossover (MDI/MDIX)

Ethernet LAN 8 ports (10/100 Base-T) switch, support Auto- Crossover (MDI/MDIX)

Physical Specifications

Dimensions: 18.98" x 6.54" x 1.77" (482mm x 166 mm x 45mm, with Bracket)
9.84" x 6.54" x 1.38" (250mm x 166 mm x 35mm, non Bracket)

Power Requirement

Input: 12VDC, 1A

Operating Environment

- Operating temperature: 0 ~ 40 degrees Celsius
- Storage temperature: -20 ~ 70 degrees Celsius
- Humidity: 20 ~ 95% non-condensing

A.2 BiGuard 2 Product Specifications



Virtual Private Network

- IPSec VPN, supports up to 2 IPSec tunnels
- IPSec VPN performance is up to 4 Mbps
- PPTP VPN, support up to 4 PPTP tunnels
- PPTP VPN performance is up to 10 Mbps
- Manual key, Internet Key Exchange (IKE) authentication and Key Management
- Authentication (MD5 / SHA-1)
- DES/3DES encryption
- AES 128/192/256 encryption
- IP Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)
- IPSec VPN concentrator
- Dynamic IPSec VPN (FQDN) support
- IPSec NAT Traversal (IPSec NAT-T)
- IPSec DPD (Dead Peer Detection)
- Supports remote access and office-to-office IPSec Connections
- PPTP Server
- Netbios over VPN

Firewall

- Stateful Packet Inspection (SPI) and Denial of Service (DoS) prevention
- Packet filter un-permitted inbound (WAN)/Inbound (LAN) Internet access by IP address, port number and packet type
- Email alert and logs of attack
- MAC Address Filtering
- Intrusion detection

Content Filtering

- URL Filter settings prevent user access to certain sites on the Internet
- Java Applet/Active X/Cookie Blocking

Quality of Service Control

- Supports DiffServ approach
- Traffic prioritization and bandwidth management based-on IP protocol, port number and IP or MAC address

Web-Based Management

- Easy-to-use WEB interface
- Firmware upgradeable via WEB interface
- Local and remote management via HTTP & HTTPS

Network Protocols and Features

- Web Diagnostics
- System Logs
- PPPoE, PPTP, Big Pond and DHCP client connections to the ISP
- NAT, static routing and RIP-2
- Router Mode (NAT Disable)
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- DHCP Server
- NTP
- SMTP Client
- SNMP
- SIP Pass-through
- IGMP snooping & IGMP Proxy
- Port based VLAN Bridge mode
- Multiple NAT (Multiple LAN & Multiple WAN)

Physical Interface

Ethernet WAN 1 ports (10/100 Base-T), support Auto- Crossover (MDI/MDIX)

Ethernet LAN 8 ports (10/100 Base-T) switch, support Auto- Crossover (MDI/MDIX)

Physical Specifications

Dimensions: 10.43" x 6.93" x 1.73" (265mm x 176 mm x 44mm)

Power Requirement

Input: 12VDC, 1A

Operating Environment

- Operating temperature: 0 ~ 40 degrees Celsius
- Storage temperature: -20 ~ 70 degrees Celsius
- Humidity: 20 ~ 95% non-condensing

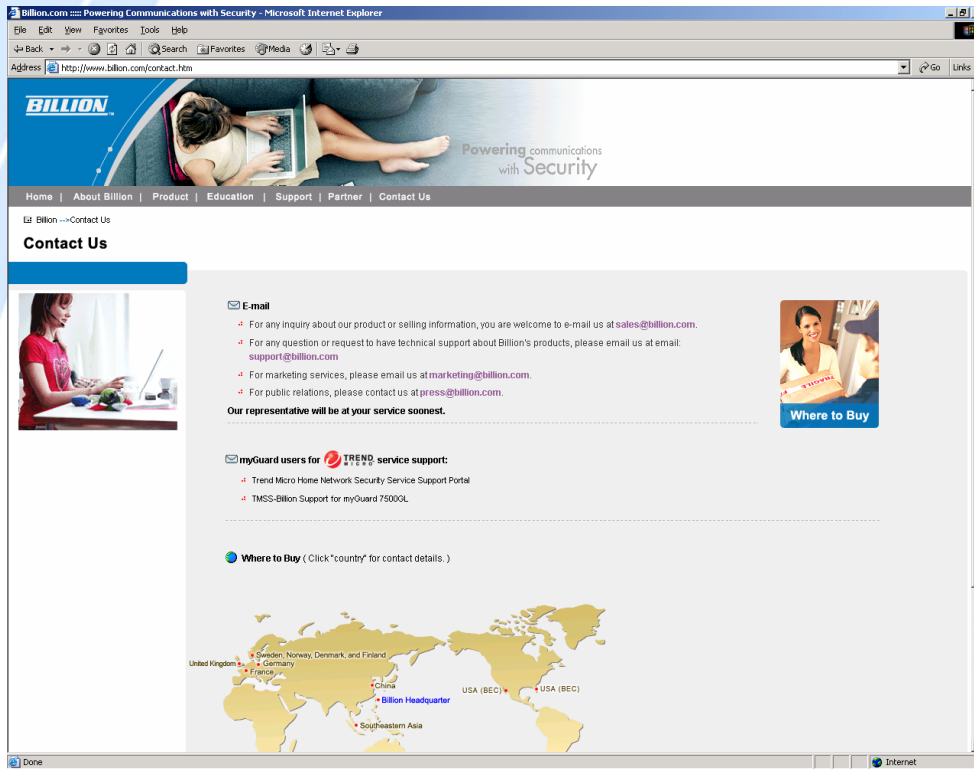
Appendix B: Customer Support

Most problems can be solved by referring to the Troubleshooting section in the User's Manual. If you cannot resolve the problem with the Troubleshooting chapter, please contact the dealer where you purchased this product.

Contact Billion

Worldwide

<http://www.billion.com/>



Appendix C: FCC Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply within the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Appendix D: Network, Routing, and Firewall Basics

D.1 Network Basics

D.1.1 IP Addresses

With the number of TCP/IP networks interconnected across the globe, ensuring that transmitted data reaches the correct destination requires each computer on the Internet has a unique identifier. This identifier is known as the IP address. The Internet Protocol (IP) uses a 32-bit address structure, and the address is usually written in dot notation.

A typical IP address looks like this:

198.25.12.8

The 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, while the second part identifies the host node or station on the network. How the address is divided depends on the address range and the application.

The five standard IP address classes each have different methods to determine the network and host sections of the address, which makes multiple hosts on a network possible. TCP/IP software identifies each address class by reading a unique bit pattern that precedes each address type. Once the address class has been recognized, the software can then correctly determine the addresses' host section. With this structure, IP addresses can uniquely identify each network and node.

D.1.1.1 Netmask

With each address class, the size of the two subdivided parts (network address and host address) is implied by the class. A net mask associated with an IP address can also express this partitioning. A net mask 32-bit quantity yields the network address when combined with an IP address. As an example, the net masks for Class A, B, and C are 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively.

Instead of dotted-decimal notation, the net mask can also be written in terms of the number of ones from the left. This number is added to the IP address, following a back slash (/). For example, a typical Class C address could be written as

192.168.234.245/24, which means that the net mask is 24 ones followed by 8 zeros. (11111111 11111111 11111111 00000000).

D.1.1.2 Subnet Addressing

Subnet addressing enables the split of one IP network address into multiple physical networks. These smaller networks are called subnetworks, and these subnetworks can make efficient use of each address when compared to needing a different network number at each end of a routed link. This technique is especially useful in smaller network environments, such as small office LANs.

A Class B address provides 16 bits of node numbers, which enable 65,536 nodes. Since most organizations don't require such a large number of nodes, the free bits can be reassigned with subnet addressing.

Multiple Class C addresses can be made from a Class B address. For example, the IP address of 172.20.0.0 allows eight extra bits to use as a subnet address, since node addresses are limited to a maximum of 255. The IP address of 172.20.52.212 would be read as IP network address 172.20, subnet number 52, and node number 212.

Besides extending the number of available addresses, this technique also allows a network manager to design an address scheme for the network by using different subnets. This can be useful when trying to distinguish other geographical locations in the network or other departments in the organization.

D.1.1.3 Private IP Addresses

When isolated from the Internet, the hosts on your local network may be assigned IP addresses with no conflicts. However, the Internet Assigned Numbers Authority (IANA) has reserved several blocks of IP addresses for private networks. These include:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.16.255.255

192.168.0.0 - 192.168.255.255

When assigning IP addresses to your private network, be sure to use IP addresses from these ranges.

D.1.2 Network Address Translation (NAT)

Traditionally, multiple PCs that needed simultaneous Internet access also required a range of IP addresses from the Internet Service Provider (ISP). Not only was this method very costly, but the number of available IP addresses for PCs is limited. Instead, BiGuard 2/10 uses a type of address sharing called Network Address Translation to grant Internet access to several PCs on the same network through the same Internet account. This method translates internal IP addresses to a single address that is unique on the Internet. This unique address can either be fixed or dynamic, depending on the type of Internet account, and the internal LAN IP addresses may also be either private or registered addresses.

NAT also offers firewall-like protection to your network, since internal LAN addresses are shielded from the public Internet. All incoming traffic to the public IP address is handled by the router, which means added security for your network from intruders. If a particular PC on your LAN requires access from outside PCs, you can use port forwarding to accomplish this. For information on how to configure port forwarding on BiGuard 2/10, refer to the **Virtual Server** section of **Chapter 4: Router Configuration**.

D.1.3 Dynamic Host Configuration Protocol (DHCP)

If the PCs on a LAN require access to the Internet, each PC must be configured with an IP address, a gateway address, and one or more DNS server addresses. Rather than configuring each PC manually, you can instead configure a network device to act as a Dynamic Host Configuration Protocol (DHCP) server. PCs on the network can automatically obtain IP addresses from a list of addresses stored on the DHCP server. In addition, other information such as gateway and DNS address can also be assigned with a DHCP server. When connecting to the ISP, BiGuard 2/10 also functions as a DHCP client. BiGuard 2/10 can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.

D.2 Router Basics

D.2.1 What is a Router?

A router is a device that forwards data packets along networks. A router is

connected to at least two networks. Usually, this is a LAN and a WAN that is connected to an ISP network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols to communicate with each other and configure the best route between any two hosts.

Routers can vary in performance and scale, the types of physical WAN connection they support, and the number of routing protocols supported. BiGuard 2/10 offers a convenient and powerful way for small-to-medium businesses to connect their networks.

D.2.2 Why use a Router?

While large bandwidth can easily and inexpensively be provided in a LAN, having high bandwidth between a LAN and the Internet can be prohibitively expensive. Because of this, Internet access is usually done through a slower WAN link, such as a cable or DSL modem. To efficiently use this slower connection, a router acts as a mechanism for selecting and transmitting data meant for the Internet. By using a router, organizations can enjoy relatively inexpensive Internet access, while maintaining a high-speed local area network.

D.2.3 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is an interior gateway protocol that specifies how routers exchange routing table information. Routers periodically update each other with RIP, changing their routing tables when necessary.

BiGuard 2/10 supports the RIP protocol. RIP also supports subnet and multicast protocols. RIP is not required for most home applications.

D.3 Firewall Basics

D.3.1 What is a Firewall?

Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. With the functionality of a NAT router, the

firewall adds features that deal with outside Internet intrusion and attacks. When an attack or intrusion is detected, the firewall can be configured to log the intrusion attempt, and can also notify the administrator of the incident. With this information, the administrator can work with the ISP to take action against the hacker. Against some types of attacks, the firewall can discard intruder packets, thereby fending off the hacker from the private network.

D.3.1.1 Stateful Packet Inspection

BiGuard 2/10 uses Stateful Packet Inspection (SPI) to protect your network from intrusions and attacks. Unlike less sophisticated Internet sharing routers, SPI ensures secure firewall filtering by intercepting incoming packets at the network layer, and analyzing them for state-related information that is associated with all network connections. User-level applications such as Web browsers and FTP can make complex network traffic patterns, which BiGuard 2/10 analyzes by looking at groups of connection states.

All state information is stored in a central cache. Traffic passing through the firewall is analyzed against these states, and then is either allowed to pass through or rejected.

D.3.1.2 Denial of Service (DoS) Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

D.3.2 Why Use a Firewall?

With a LAN connected to the Internet through a router, there is a chance for hackers to access or disrupt your network. A simple NAT router provides a basic level of protection by shielding your network from the outside Internet. Still, there are ways for more dedicated hackers to either obtain information about your network or disrupt your network's Internet access. Your BiGuard 2/10 provides an extra level of protection from such attacks with its built-in firewall.

Appendix E: Virtual Private Networking

E.1 What is a VPN?

A Virtual Private Network (VPN) is a shared network where private data is segmented from other traffic so that only the intended recipient has access. It allows organizations to securely transmit data over a public medium like the Internet. VPNs utilize tunnels, which allow data to be safely delivered to the intended recipient.

Because private networks lack data security, IPSec-based VPNs employ encryption technologies that protect a private network from data theft or tampering. These private networks can be implemented over any type of IP network, which allows for excellent flexibility.

E.1.1 VPN Applications

VPNs are traditionally used three ways:

- Extranets: Extranets are secure connections between two or more organizations. IPSec-based VPNs are ideal for extranet connections, as they can be quickly and inexpensively installed. Extranets are often used to securely share a company's information with suppliers, vendors, customers, or other businesses.
- Intranets: Intranets are private networks that connect an organization's locations together. These locations range from a headquarter, to branch offices, to a remote employee's home. Intranets are often used for email and for sharing applications and files. A firewall protects Intranets from unauthorized access.
- Remote Access: Remote access enables mobile workers to access email and business applications. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.

E.2 What is IPSec?

Internet Protocol Security (IPSec) is a set of protocols and algorithms that provide data authentication, integrity, and confidentiality as data is transferred across IP networks. IPSec provides data security at the IP packet level, and protects against possible security risks by protecting data. IPSec is widely used to establish VPNs.

There are three major functions of IPSec:

- Confidentiality: Conceals data through encryption.
- Integrity: Ensures that contents did not change in transit.
- Authentication: Verifies that packets received are actually from the claimed sender.

E.2.1 IPSec Security Components

IPSec contains three major components:

- Authentication Header (AH): Provides authentication and integrity.
- Encapsulating Security Payload (ESP): Provides confidentiality, authentication, and integrity.
- Internet Key Exchange (IKE): Provides key management and Security Association (SA) management.

These components are discussed below.

E.2.1.1 Authentication Header (AH)

The Authentication Header (AH) is a protocol that provides authentication and integrity, protecting data from tampering. It provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram.

The AH can also protect packets from unauthorized re-transmission with anti-replay functionality. The presence of the AH header allows us to verify the integrity of the message, but doesn't encrypt it. Thus, AH provides authentication but not privacy. ESP protects data confidentiality. Both AH and ESP can be used together for added protection.

A typical AH packet looks like this:

Next Header	Payload Length	Reserved
SPI		
Sequence Number		
Authentication Data		

E.2.1.2 Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) provides privacy for data through encryption. An encryption algorithm combines the data with a key to encrypt it. It then repackages the data using a special format, and transmits it to the destination. The receiver then decrypts the data using the same algorithm. ESP is usually used with AH to provide added data security.

ESP divides its fields into three components...

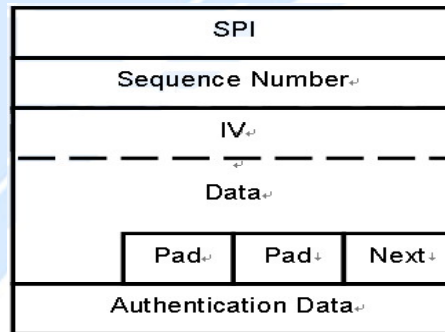
ESP Header: Placed before encrypted data, the ESP Header contains the SPI and Sequence Number. Its placement depends on whether ESP is used in transport mode or tunnel mode.

ESP Trailer: Placed after the encrypted data, the ESP Trailer contains padding that is used to align the encrypted data.

ESP Authentication Data: This contains an Integrity Check Value (ICV) for when ESP's optional authentication feature is used.

ESP provides authentication, integrity, and confidentiality, which provides data content protection, and protects against data tampering. A typical ESP packet looks

like this:



E.2.1.3 Security Associations (SA)

Security Associations are a one-way relationships between sender and receiver that specify IPsec-related parameters. They provide data protection by using the defined IPsec protocols, and allow organizations to control according to the security policy in effect, which resources may communicate securely.

SA is identified by 3 parameters:

- Security Parameters Index (SPI), a locally unique value
- Destination IP Address
- Security Protocol: (AH or ESP, but not both)

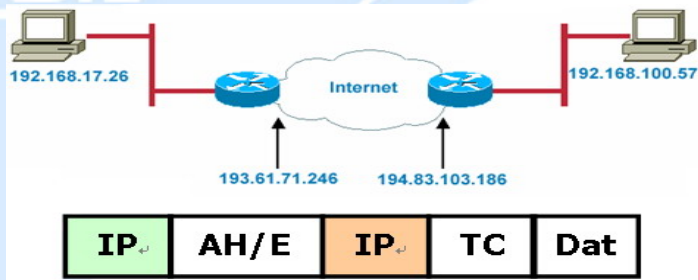
There are several other parameters associated with an SA that are stored in a Security Association database.

E.2.2 IPsec Modes

To exchange data between different types of VPNs, IPsec provides two major modes:

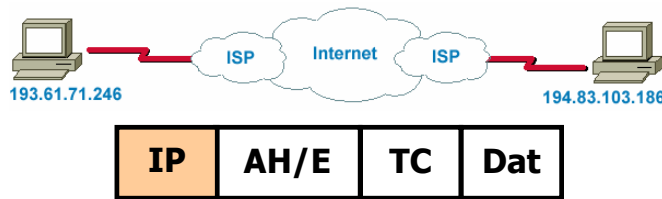
- Tunnel Mode :

This mode is used for host-to-host security. Protection extends to the payload of IP data, and the IP addresses of the hosts must be public IP addresses.



Transport Mode :

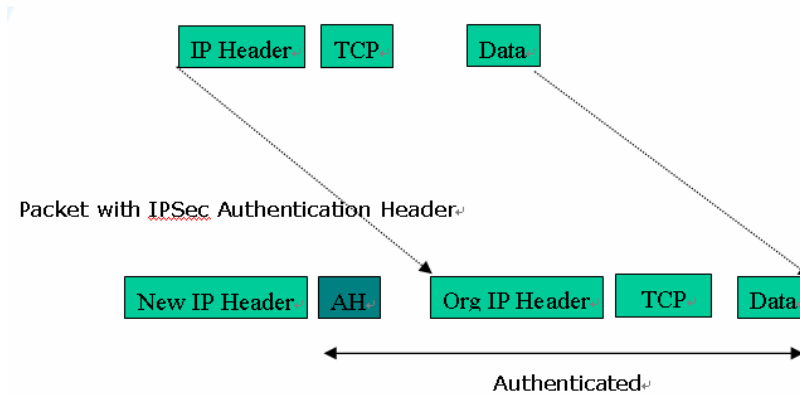
- This mode is used to provide data security between two networks. It provides protection for the entire IP packet and is sent by adding an outer IP header corresponding to the two tunnel end-points. Since tunnel mode hides the original IP header, it provides security of the networks with private IP address space.



E.2.3 Tunnel Mode AH

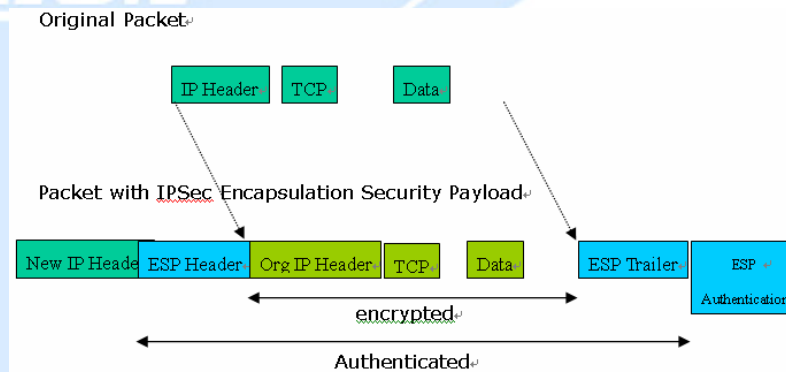
AH is typically applied to a data packet in the following manner:

Original Packet:



E.2.4 Tunnel Mode ESP

Here is an example of a packet with ESP applied:



E.2.5 Internet Key Exchange (IKE)

Before either AH or ESP can be used, it is necessary for the two communication devices to exchange a secret key that the security protocols themselves will use. To do this, IPsec uses Internet Key Exchange (IKE) as a primary support protocol. IKE facilitates and automates the SA setup, and exchanges keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it. These keys need to be re-created or refreshed frequently so that the parties can communicate securely with each other. Refreshing keys on a regular basis ensures data confidentiality.

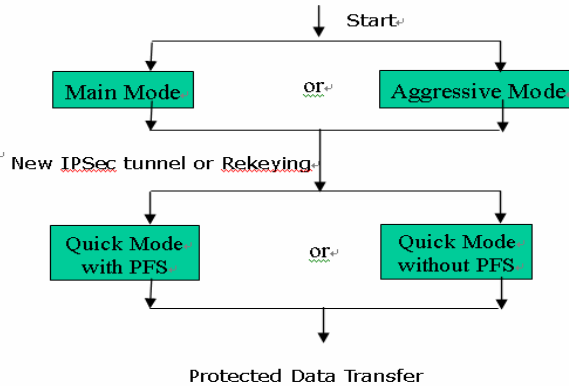
There are two phases to this process. Phase I deals with the negotiation and management of IKE and IPsec parameters. This phase can be carried out in either one of two modes: Main Mode or Aggressive Mode. Main mode utilizes three message pairs that negotiate IKE parameters, establish a shared secret and derive session keys, and exchange and provide identities, retroactively authenticating the information sent. This method is very secure, but when using the pre-shared key method for authentication, it is possible to use IDs other than the packets's IP addresses. Aggressive mode reduces this process to three messages, but parameter negotiation is limited, identity protection is lacking except when using public key encryption, and is more vulnerable to Denial of Service attacks.

Phase II, known as Quick Mode, establishes symmetrical IPsec Security Associations for both AH and ESP. It does this by negotiating IPsec parameters, exchange nonces to derive session keys from the IKE shared secret, exchange DH values to generate a new key, and identify which traffic this SA bundle will protect using selectors (IDi and IDr payloads).

The following is an illustration on how data is handled with IKE:

Phase 1
Negotiate
ISAKMP SA
Mutual Authentication

Phase 2
Negotiate SAs
for AH and ESP



Appendix F: IPsec Logs and Events

F.1 IPsec Log Event Categories

There are three major categories of IPsec Log Events for your BiGuard 2/10. These include:

1. IKE Negotiate Packet Messages
2. Rejected IKE Messages
3. IKE Negotiated Status Messages

The table in the following section lists the different events of each category, and provides a detailed explanation of each.

F.2 IPsec Log Event Table

IKE Negotiate Packet Messages	
Log Event	Explanation
Send Main mode initial message of ISAKMP	Sending the first initial message of main mode (phase I). Done to exchange encryption algorithm, hash algorithm, and authentication method.
Send Aggressive mode initial message of ISAKMP	Sending the first message of aggressive mode (phase I).
Received Main mode initial message of ISAKMP	Received the first message of main mode.
Send Main mode first response message of ISAKMP	Sending the first response message of main mode. Done to exchange encryption algorithm, hash algorithm, and authentication method.
Received Main mode first response message of ISAKMP	Received the first response message of main mode. Done to exchange encryption algorithm, hash algorithm, and authentication method.
Send Main mode second message of ISAKMP	Sending the second message of main mode. Done to exchange key values.
Received Main mode second message of ISAKMP	Received the second message of main mode. Done to exchange key values.

Send Main mode second response message of ISAKMP	Sending the main mode second response message. Done to exchange key values.
Received Main mode second response message of ISAKMP	Received the main mode second response message. Done to exchange key values.
Send Main mode third message of ISAKMP	Sending the third message of main mode. Done for authentication.
Received Main mode third message of ISAKMP	Received the third message of main mode. Done for authentication.
Send Main mode third response message of ISAKMP	Sending the third response message of main mode. Done for authentication.\
Received Main mode third response message of ISAKMP	Received the third response message of main mode. Done for authentication.
Received Aggressive mode initial ISAKMP Message	Received the first message of aggressive mode.
Send Aggressive mode first response message of ISAKMP	Sending the first response message of aggressive mode. Done to exchange proposal and key values.
Received Aggressive mode first response message of ISAKMP	Received the first response message of aggressive mode. Done to exchange proposal and key values.
Send Aggressive mode second message of ISAKMP	Sending the second message of aggressive mode. Done to exchange proposal and key values.
Received Aggressive mode second ISAKP Message	Received the second message of aggressive mode. Done to exchange proposal and key values.
Send Quick mode initial message	Sending the first message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Received Quick mode initial message	Received the first message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Send Quick mode first response message	Sending the first response message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).

Received Quick mode first response message	Received the first response message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Send Quick mode second message	Sending the second message of quick mode (Phase II).
Received Quick mode second message	Received the second message of quick mode (Phase II).
ISAKMP IKE Packet	Indicates IKE packet.
ISAKMP Information	Indicates Information packet.
ISAKMP Quick Mode	Indicates quick mode packet.
Rejected IKE Messages	
NO PROPOSAL CHOSEN: No acceptable Oakley Transform	
NO PROPOSAL CHOSEN: No acceptable Proposal in IPsec SA	
NO PROPOSAL CHOSEN: PFS is required in Quick Initial SA.	
NO PROPOSAL CHOSEN: PFS is not required in Quick Initial SA.	
NO PROPOSAL CHOSEN: Initial Aggressive Mode message from %s but no connection has been configured	
NO PROPOSAL CHOSEN: Initial Main Mode message received on %s:%u but no connection has been authorized	
INVALID ID: Require peer to have ID %s, but peer declares %s	
INVALID ID INFORMATION: Initial Aggressive Mode packet claiming to be from %s on %s but no connection has been authorized	
INVALID ID: Require peer to have ID %s, but peer declares %s	
INVALID ID INFORMATION: Initial Aggressive Mode packet claiming to be from %s on %s but no connection has been authorized	
IKE Negotiated Status Messages	
Received Delete SA payload and deleting IPSEC State (<i>integer</i>)	
Received Delete SA payload: Deleting ISAKMP State (<i>integer</i>)	

(Main/Aggressive) mode peer ID is (identifier string)
ISAKMP SA Established
IPsec SA Established

Appendix G: Bandwidth Management with QoS

G.1 Overview

In a home or office environment, users constantly have to transmit data to and from the Internet. When too many are accessing the Internet at the same time, service can slow to a crawl, causing service interruptions and general frustration. Quality of Service (QoS) is one of the ways BiGuard 2/10 can optimize the use of bandwidth, ensuring a smooth and responsive Internet connection for all users.

G.2 What is Quality of Service?

QoS is a feature that prioritizes and guarantees bandwidth to achieve optimal service performance. QoS can maximize the use of available network bandwidth by prioritizing time-sensitive traffic to avoid latencies and delays. By ensuring that time-sensitive applications such as VoIP and streaming video get priority access to bandwidth, users in both home and office environments can enjoy smooth and responsive data transmission no matter which applications they are running.

If you've ever experienced slow Internet speeds due to other network users using bandwidth-consuming applications like P2P, you'll understand why QoS is such a breakthrough for home users and office users. Billion makes itself unique by integrating QoS in its routers for both inbound and outbound traffic.

QoS helps users manage bandwidth and effectively prioritize data traffic. It gives you full control over the traffic of any type of data. Employed on DiffServ (Differentiated Services) architecture, data traffic is given priority by the router; ensuring latency-sensitive applications like voice and mission-critical data such as VPN move through the router at lightning speeds, even under heavy load. You can throttle the speed of different types of data passing through the router, limit the speed of unimportant or bandwidth-consuming applications, and even distribute the bandwidth for different groups of users at home or in the office. QoS keeps your Internet connection smooth and responsive.

G.3 How Does QoS Work?

QoS employs three different methods for optimizing bandwidth:

- Prioritization: Assigns different priority levels for different applications, prioritizing traffic. High, Normal and Low priority settings.
- Outbound and Inbound IP Throttling: Controls network traffic and allows you to limit the speed of each application.
- DiffServ Technology: Manages priority queues and DSCP tagging through the Internet backbone. Manages traffic among Ethernet, wireless, and ADSL interfaces.

G.4 Who Needs QoS?

QoS is ideal for home and office users who need to use a variety of real-time applications like VoIP, on-line games, P2P, video streaming, and FTP simultaneously. With QoS, you can optimize your bandwidth to accommodate several of these applications without experiencing latency or service interruptions.

G.4.1 Home Users

Low latency is everything for gamers. Most home users feel frustrated when trying to play an online game over a shared ADSL connection. Unfortunately, most routers have no way of determining the importance of the packet at any given time. All the traffic is treated equally, so a packet containing an "urgent" command may be delayed. QoS gives you the ability to control the bandwidth. Using IP Throttling, bandwidth limits can be enforced on a particular application or any system within the LAN. Prioritization specifies which packets have priority and should not be delayed, and which packets have lower priority and should be moved to the end of the upload queue.

Suppose there are four students sharing a three-floor house with one single broadband connection. Tom, a college freshman, is playing the online game with his group members, while Mary, a sophomore student, is talking to her net pal via Skype. Meanwhile, Jacky is downloading a movie file by using the P2P application program. Sophia, however, is just trying to log on to the website to send her photos to her family. As a result, the net speed slows to a crawl and affects everyone sharing the Internet connection. QoS is designed for managing traffic flow and bandwidth to solve this problem. You can first classify different applications (online games, FTP, Skype, email) as shown in the table below. Then, you can manage and prioritize the flow of bandwidth at different levels (e.g. 30% for games, 20% for downloads, 10% for email, 20% for FTP, and 35% for others). QoS can be used to identify different applications and assign priority to enable a smooth and responsive

Application	Data Ratio (%)	Priority
On-line games	30%	High
Skype	5%	High
Email	10%	High
FTP	20%	Upload (High), Download (Normal)
Other	35%	

G.4.2 Office Users

QoS is also ideal for small businesses using an office server as a web server. With QoS control, web pages served to your customers can be given top priority and delivered first so that it will not be impeded by email and office web browsing.

Here is a good example of how QoS can work in an office environment. A CEO is holding a videoconference with international clients in the meeting room. However, the streaming video and voice frequently lag. Sales people are talking to international agencies via VoIP phone, while sending orders via email to vendors for production. However, some staff are downloading MP3 music files, large-size photos and watching video streaming online. Consequently, the Internet connection slows down. This is why business users need QoS to manage data traffic. With QoS, the network administrator can define and classify important packets; specify a minimum guaranteed rate for each application, and ensure that important packets have priority to ensure a good quality of broadband connection for the entire organization.

Application	Data Ratio (%)	Priority
Videoconferencing	30%	High
VoIP	20%	High
Email	10%	High

BILLION

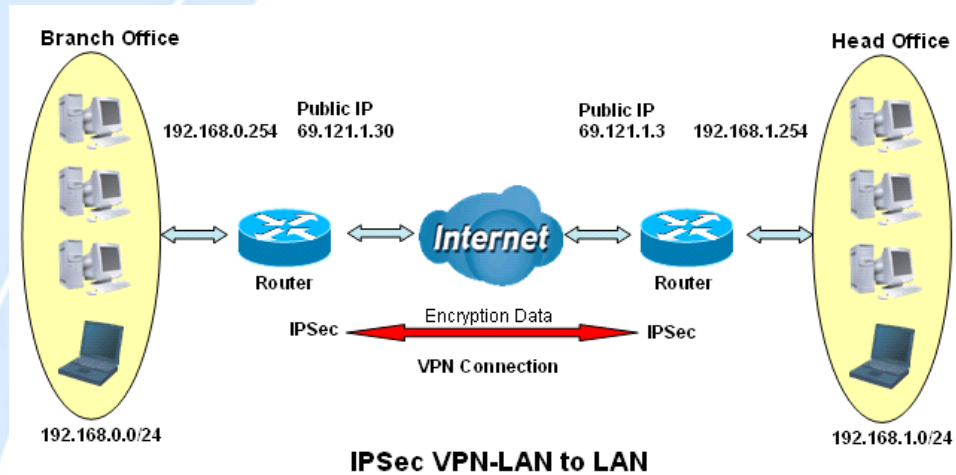
FTP	10%	Upload (High), Download (Normal)
Other	30%	MP3 (Low), MSN (Normal)

Appendix H: Router Setup Examples

H.1 VPN Configuration

This section outlines some concrete examples on how you can configure BiGuard 2/10 for your VPN.

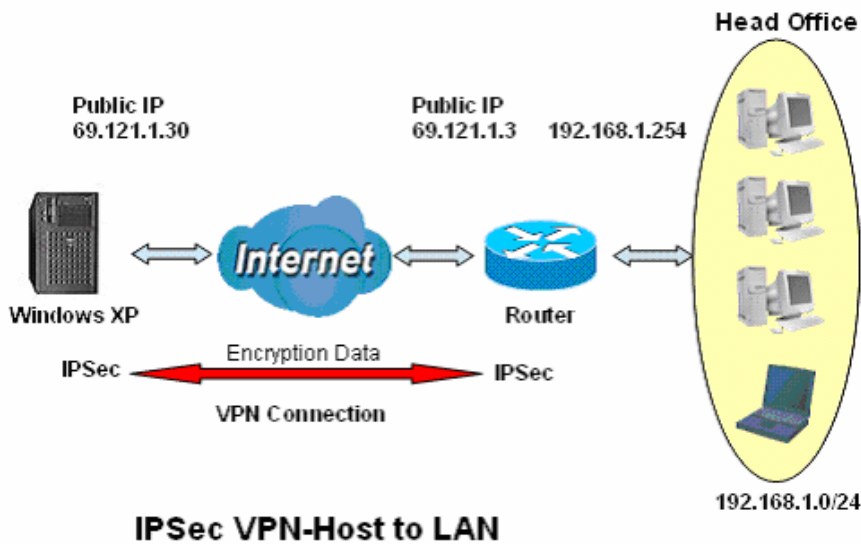
H.1.1 LAN to LAN



	Branch Office	Head Office
Local		
ID	IP Address	IP Address
Data	69.121.1.30	69.121.1.3
Network	Any Local Address	Any Local Address
IP Address	192.168.0.0	192.168.1.0
Netmask	255.255.255.0	255.255.255.0
Remote		
Secure Gateway Address(or Hostname)	69.121.1.3	69.121.1.30

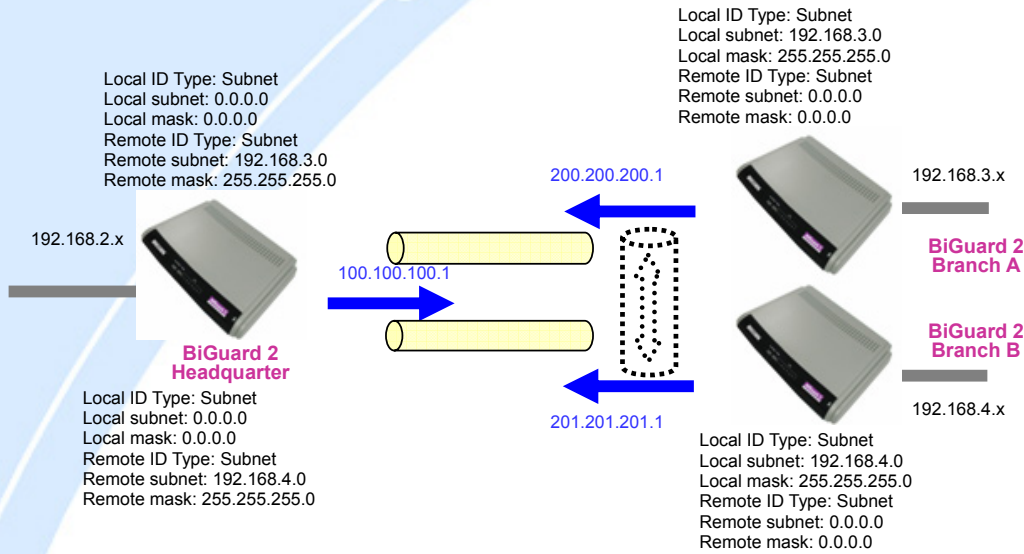
ID	IP Address	IP Address
Data	69.121.1.3	69.121.1.30
Network	Subnet	Subnet
IP Address	192.168.1.0	192.168.0.0
Netmask	255.255.255.0	255.255.255.0
Proposal		
IKE Pre-shared Key	12345678	12345678
Security Algorithm	Main Mode; ESP: MD5 3DES PFS	Main ESP MD5 3DES PFS

H.1.2 Host to LAN



	Single client	Head Office
Local		
ID	IP Address	IP Address
Data	69.121.1.30	69.121.1.3
Network	Any Local Address	Any Local Address
IP Address	0.0.0.0	192.168.1.0
Netmask	0.0.0.0	255.255.255.0
Remote		
Secure Gateway Address(or Hostname)	69.121.1.3	69.121.1.30
ID	IP Address	IP Address
Data	69.121.1.3	69.121.1.30
Network	Subnet	Single Address
IP Address	192.168.1.0	69.121.1.30
Netmask	255.255.255.0	255.255.255.255
Proposal		
IKE Pre-shared Key	12345678	12345678
Security Algorithm	Main Mode; ESP: MD5 3DES PFS	Main ESP MD5 3DES PFS

H.2 VPN Concentrator



Step 1: Go to **Configuration > IPSec** and configure the link from BiGuard 2/10 Headquarter to BiGuard 2/10 Branch A.

Status	Connection Name	test1	
Quick Start	Tunnel	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Configuration	Local		
LAN	ID	IP Address	100.100.100.1
WAN	Network	IP Address	0 . 0 . 0 . 0
Bandwidth Settings		End IP Address	0 . 0 . 0 . 0
System		Netmask	0 . 0 . 0 . 0
Firewall	Remote		
VPN	Secure Gateway	IP Address/ Hostname	200.200.200.1
IPSec	ID	Remote WAN IP	200.200.200.1
IPSec Wizard	Network	IP Address	192 . 168 . 3 . 0
IPSec Policy		End IP Address	0 . 0 . 0 . 0
PPTP		Netmask	255 . 255 . 255 . 0
QoS	Proposal		
Virtual Server	Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key	
Advanced	Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH	
Save Config to Flash	Encryption Protocol	3DES	
	Authentication Protocol	MD5	
	Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
	PreShared Key	12345678	
	IKE Life Time	28800	Seconds
	Key Life Time	3600	Seconds
	Netbios Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
	Annly		
	<input type="button" value="SAVE CONFIG"/> <input type="button" value="RESTART"/> <input type="button" value="LOGOUT"/>		

Step 2: Go to **Configuration > IPSec** and configure the link from BiGuard 2/10 Headquarter to BiGuard 2/10 Branch B.

<ul style="list-style-type: none"> Status Quick Start Configuration LAN WAN Bandwidth Settings System Firewall VPN IPSec IPSec Wizard IPSec Policy PPTP QoS Virtual Server Advanced Save Config to Flash 	Connection Name	test2				
	Tunnel	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				
	Local					
	ID	IP Address	Data		100.100.100.1	
	Network	IP Address	0	0	0	0
		End IP Address	0	0	0	0
		Netmask	0	0	0	0
	Remote					
	Secure Gateway	IP Address/ Hostname	Data		201.201.201.1	
	ID	Remote WAN IP	Data		201.201.201.1	
	Network	IP Address	192	168	4	0
		End IP Address	0	0	0	0
		Netmask	255	255	255	0
	Proposal					
	Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key				
	Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH				
	Encryption Protocol	3DES				
	Authentication Protocol	MD5				
	Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				
	PreShared Key	12345678				
IKE Life Time	26800	Seconds				
Key Life Time	3600	Seconds				
Netbios Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled					
Apply						
<input type="button" value="SAVE CONFIG"/> <input type="button" value="RESTART"/> <input type="button" value="LOGOUT"/>						

Step 3: Go to **Configuration > IPSec** and configure the connection from BiGuard 2/10 Branch A to BiGuard 2/10 Headquarter.

<ul style="list-style-type: none"> Status Quick Start Configuration LAN WAN Bandwidth Settings System Firewall VPN IPSec IPSec Wizard IPSec Policy PPTP QoS Virtual Server Advanced Save Config to Flash 	Connection Name	test1				
	Tunnel	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				
	Local					
	ID	IP Address	Data		200.200.200.1	
	Network	IP Address	192	168	3	0
		End IP Address	0	0	0	0
		Netmask	255	255	255	0
	Remote					
	Secure Gateway	IP Address/ Hostname	Data		100.100.100.1	
	ID	Remote WAN IP	Data		100.100.100.1	
	Network	IP Address	0	0	0	0
		End IP Address	0	0	0	0
		Netmask	0	0	0	0
	Proposal					
	Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key				
	Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH				
	Encryption Protocol	3DES				
	Authentication Protocol	MD5				
	Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled				
	PreShared Key	12345678				
IKE Life Time	26800	Seconds				
Key Life Time	3600	Seconds				
Netbios Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled					
Apply						
<input type="button" value="SAVE CONFIG"/> <input type="button" value="RESTART"/> <input type="button" value="LOGOUT"/>						

Step 4: Go to **Configuration > IPSec** and configure the connection from the BiGuard 2/10 Branch B to BiGuard 2/10 Headquarter.

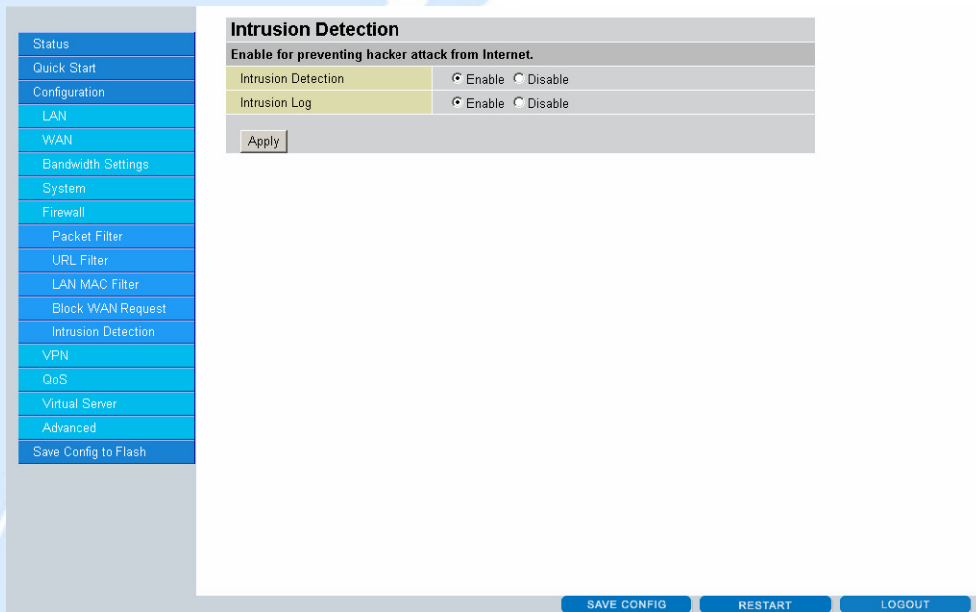
Connection Name		test1	
Tunnel		<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Local			
ID	IP Address	Data 201.201.201.1	
Network	IP Address	192	168
	End IP Address	0	0
	Netmask	255	255
Remote			
Secure Gateway	IP Address/ Hostname	Data 100.100.100.1	
ID	Remote WAN IP	Data 100.100.100.1	
Network	IP Address	0	0
	End IP Address	0	0
	Netmask	0	0
Proposal			
Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key		
Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Protocol	3DES		
Authentication Protocol	MD5		
Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
PreShared Key	12345678		
IKE Life Time	26800	Seconds	
Key Life Time	3600	Seconds	
Netbios Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
Apply			
SAVE CONFIG		RESTART	
LOGOUT			

Step 5: Click **Save Config** to save all changes to flash memory.

H.3 Intrusion Detection

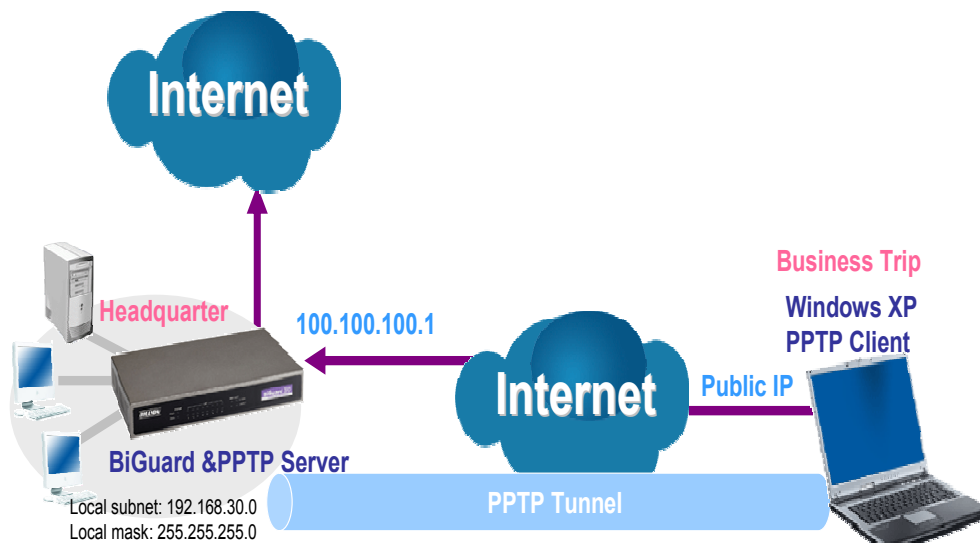


Step 1: Go to **Configuration > Firewall > Intrusion Detection** and Enable the settings.



Step 2: Click **Apply** and then **Save Config** to save all changes to flash memory.

H.4 PPTP Remote Access by Windows XP



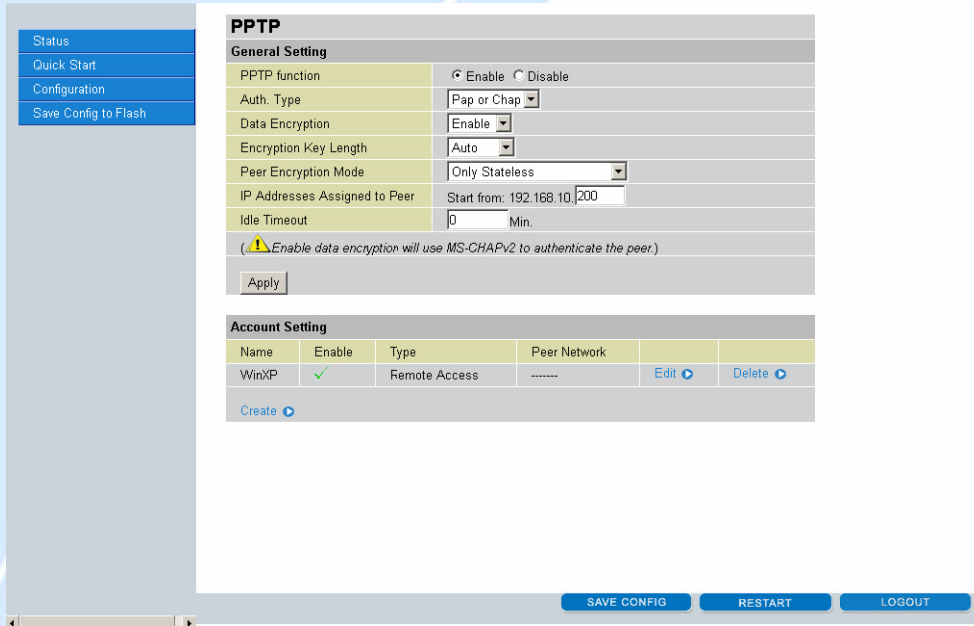
Step1: Go to **Configuration > VPN > PPTP** and Enable the PPTP function, Click **Apply**.

The screenshot shows the PPTP configuration interface. On the left is a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Bandwidth Settings, System, Firewall, VPN, IPsec, IPsec Wizard, IPsec Policy, PPTP, QoS, Virtual Server, Advanced, and Save Config to Flash. The main content area is titled 'PPTP' and contains two sections: 'General Setting' and 'Account Setting'. The 'General Setting' section includes: PPTP function (radio buttons for Enable and Disable, with 'Enable' selected), Auth. Type (dropdown menu showing 'Pap or Chap'), Data Encryption (dropdown menu showing 'Disable'), Encryption Key Length (dropdown menu showing 'Auto'), Peer Encryption Mode (dropdown menu showing 'Only Stateless'), IP Addresses Assigned to Peer (text input 'Start from: 192.168.1.200'), and Idle Timeout (text input '0' with 'Min.' label). A warning message states: '(Enable data encryption will use MS-CHAPv2 to authenticate the peer.)'. Below this is an 'Apply' button. The 'Account Setting' section is a table with columns: Name, Enable, Type, Peer Network, and an empty column. Below the table is a 'Create' button with a plus icon. At the bottom of the page are three buttons: 'SAVE CONFIG', 'RESTART', and 'LOGOUT'.

Step2: Click **Create** to create a PPTP Account.

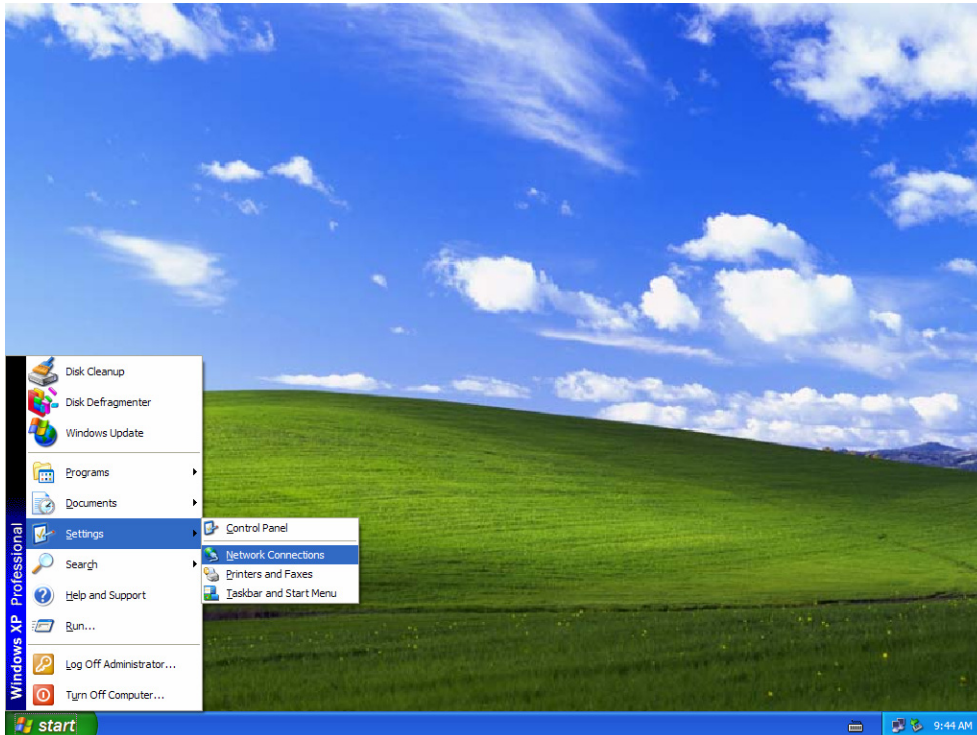
The screenshot shows the 'Add PPTP Account' configuration page. The left navigation menu is the same as in the previous screenshot. The main content area is titled 'PPTP' and contains the 'Add PPTP Account' section. It includes: Connection Name (text input 'WinXP'), Tunnel (radio buttons for Enable and Disable, with 'Enable' selected), Username (text input 'test'), Password (password field with 4 dots), Retype Password (password field with 4 dots), Connection Type (radio buttons for Remote Access and LAN to LAN, with 'Remote Access' selected), Peer Network IP (four text input fields), Peer Netmask (four text input fields), and Netbios Broadcast (radio buttons for Enable and Disable, with 'Disable' selected). Below this is an 'Apply' button. At the bottom of the page are three buttons: 'SAVE CONFIG', 'RESTART', and 'LOGOUT'.

Step3: Click **Apply**, you can see the account is successfully created.

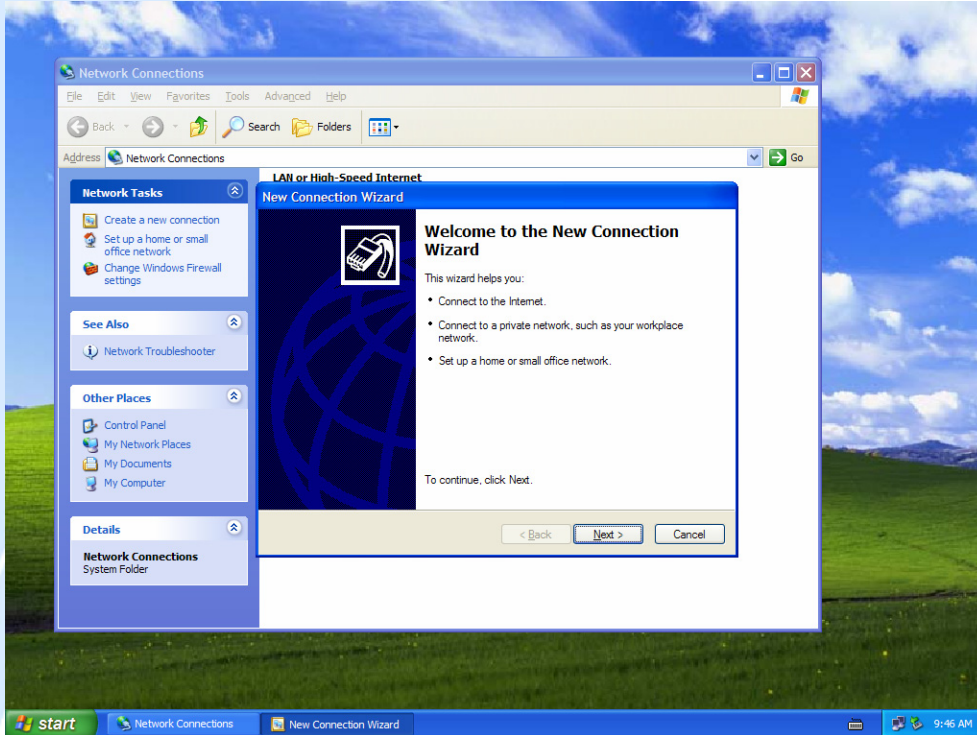


Step4: Click **Save Config** to save all changes to flash memory.

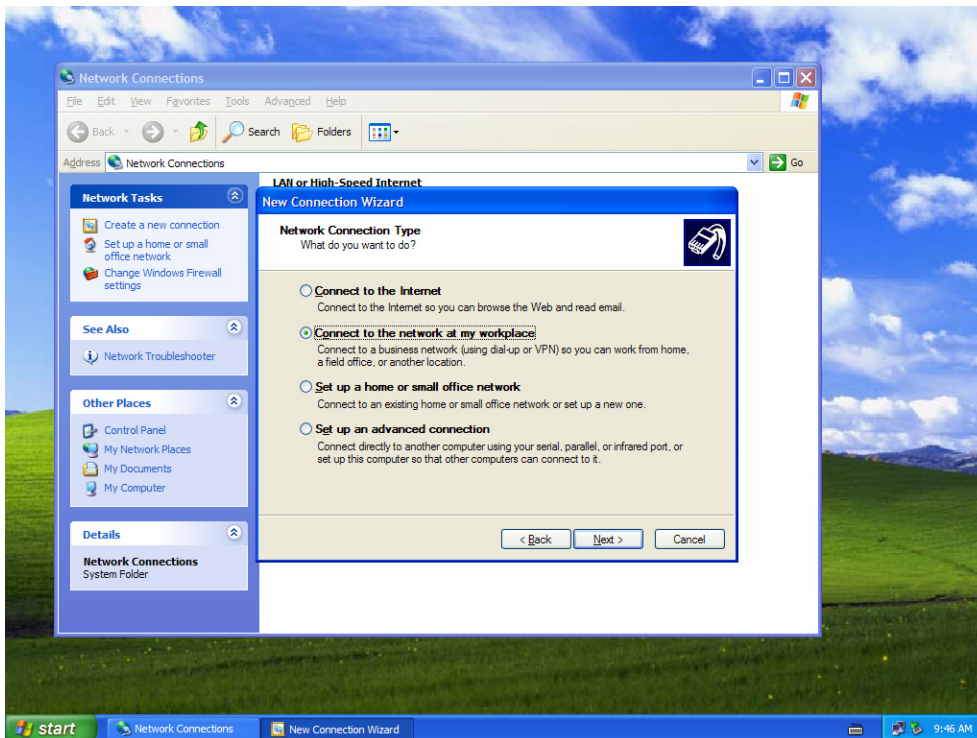
Step5: In Windows XP, go **Start > Settings > Network Connections**.



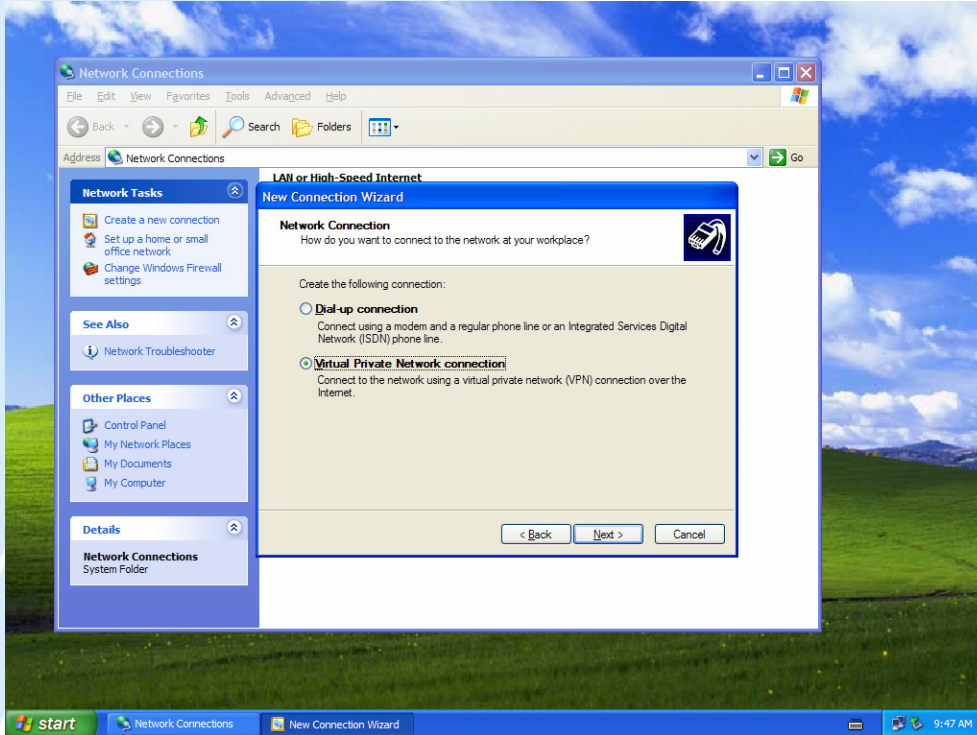
Step6: In **Network Tasks**, Click **Create a new connection**, and press **Next**.



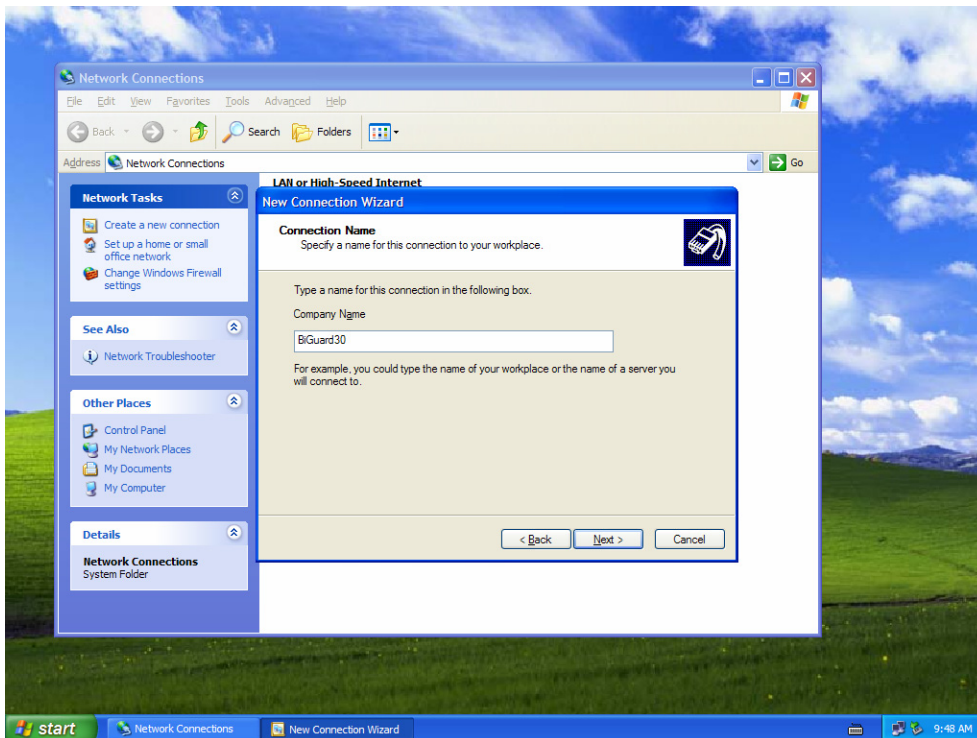
Step7: Select **Connect to the network at my workplace** and press **Next**.



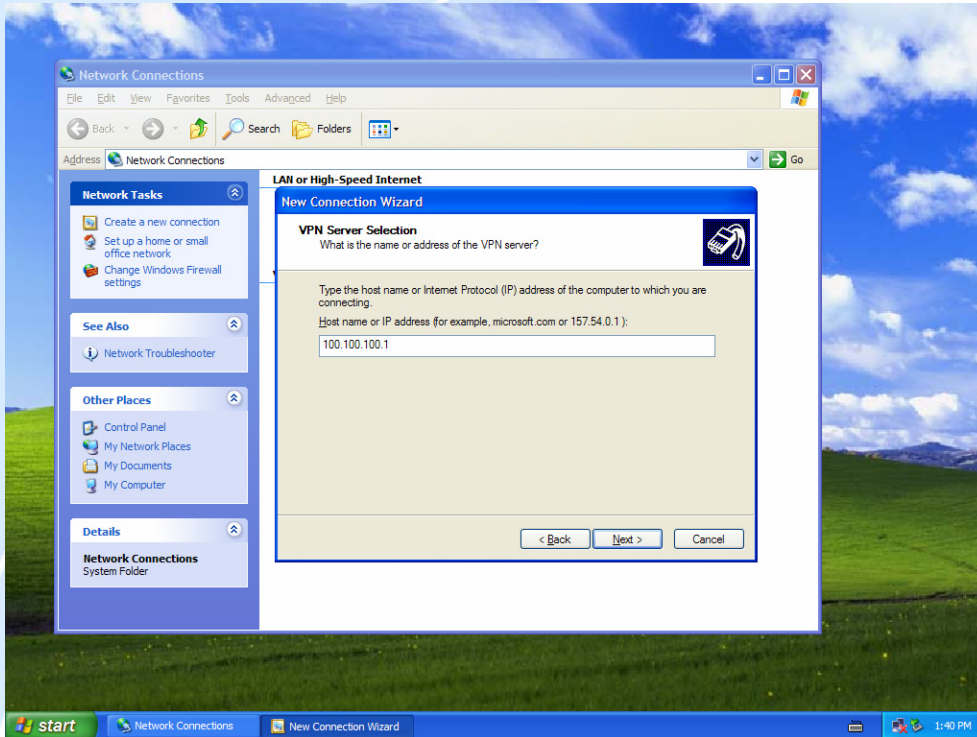
Step8: Select Virtual **Private Network connection** and press **Next**.



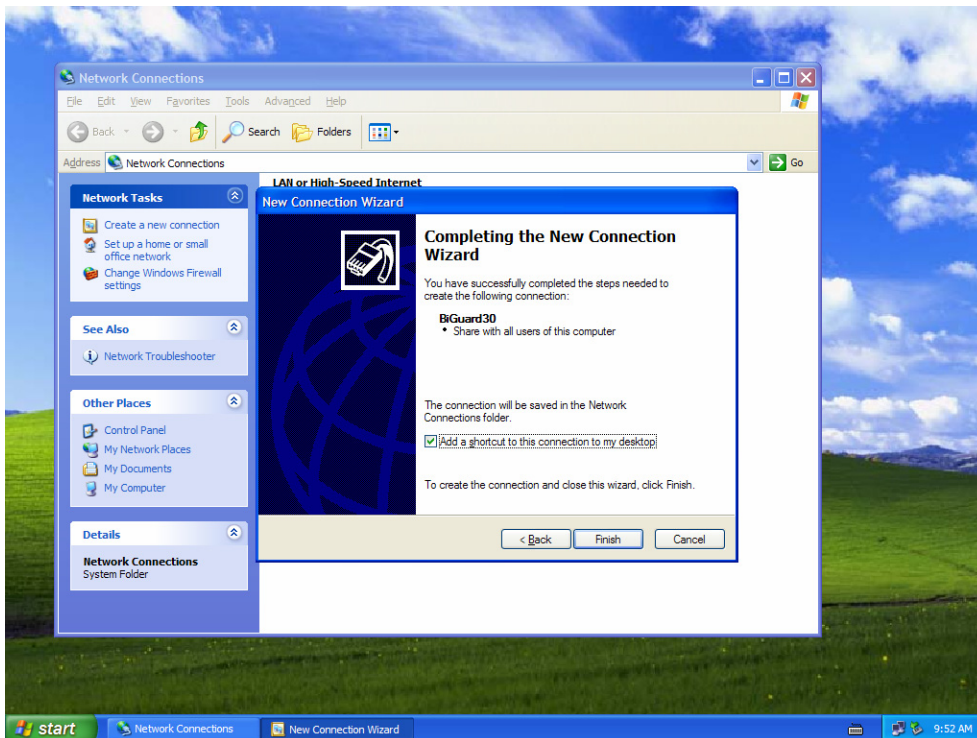
Step9: Input the user-defined name for this connection and press **Next**.



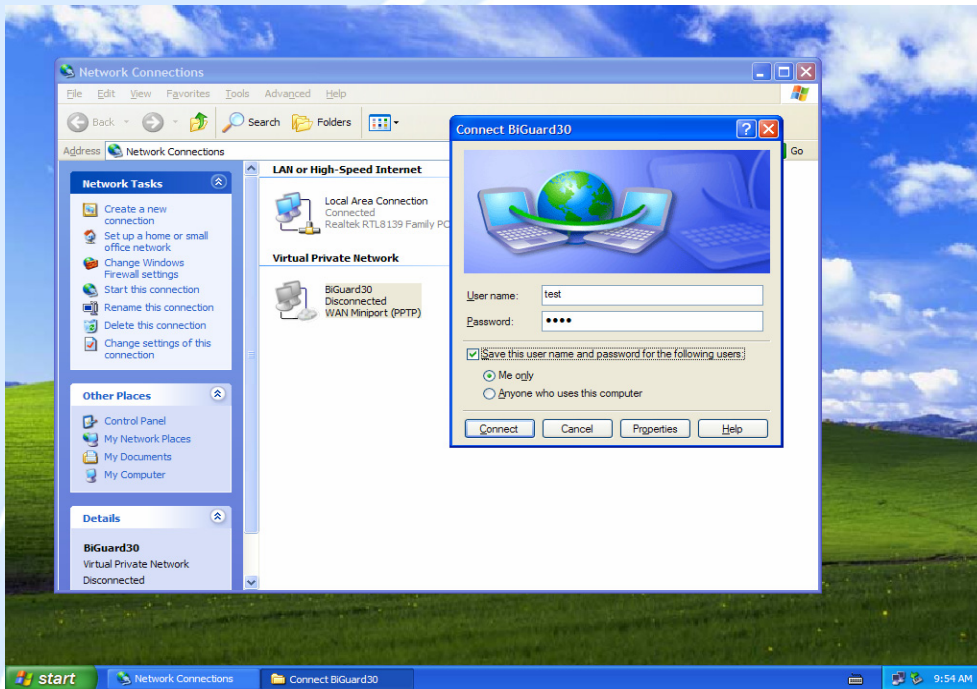
Step10: Input PPTP Server Address and press **Next**.



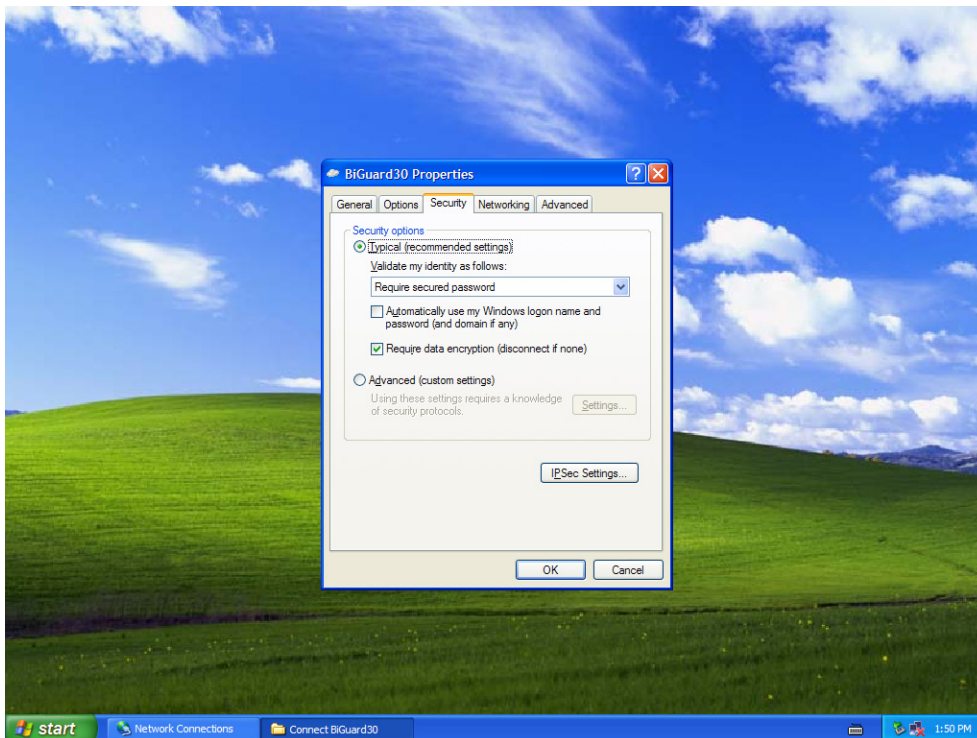
Step11: Please press **Finish**.



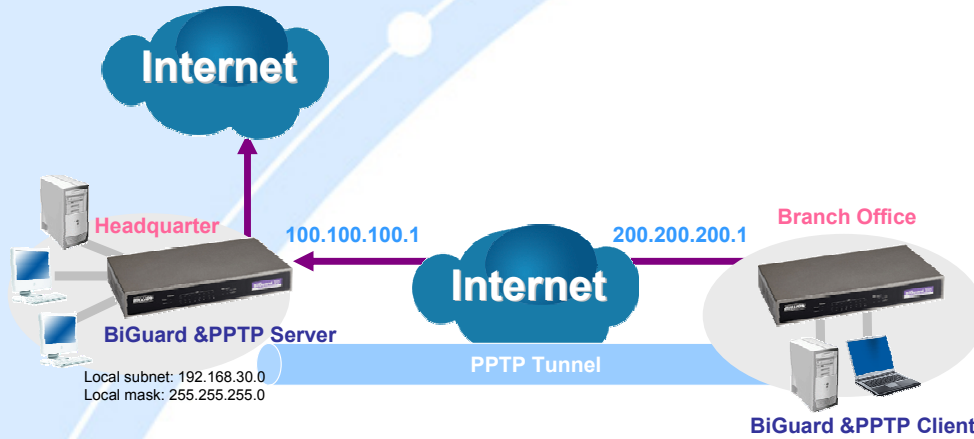
Step12: Double click the connection, and input **Username** and **Password** that defined in BiGuard PPTP **Account Settings**.



PS. You can also refer the **Properties** > **Security** page as below, by default.



H.5 PPTP Remote Access by BiGuard



Step1: Go to **Configuration > VPN > PPTP** and Enable the PPTP function, **Disable** the **Encryption**, then Click **Apply**.

The screenshot shows the **PPTP** configuration page. On the left is a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Bandwidth Settings, System, Firewall, VPN, IPsec, IPsec Wizard, IPsec Policy, PPTP, QoS, Virtual Server, Advanced, and Save Config to Flash. The main content area is titled **PPTP** and is divided into two sections:

- General Setting**:
 - PPTP function: Enable Disable
 - Auth. Type: Pap or Chap
 - Data Encryption: Enable
 - Encryption Key Length: Auto
 - Peer Encryption Mode: Only Stateless
 - IP Addresses Assigned to Peer: Start from: 192.168.1.200
 - Idle Timeout: 0 Min.
 - Warning: (⚠️ Enable data encryption will use MS-CHAPv2 to authenticate the peer.)
 - Apply button
- Account Setting**:
 - Table with columns: Name, Enable, Type, Peer Network
 - Create button

At the bottom of the page are buttons for **SAVE CONFIG**, **RESTART**, and **LOGOUT**.

Step2: Click **Create** to create a PPTP Account.

- Status
- Quick Start
- Configuration
- Save Config to Flash

PPTP

Add PPTP Account

Connection Name	BiGuard10		
Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Username	test		
Password	••••		
Retype Password	••••		
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN to LAN		
Peer Network IP	192	168	30
Peer Netmask	255	255	0
Netbios Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

Step3: Click **Apply**, you can see the account is successfully created.

- Status
- Quick Start
- Configuration
- Save Config to Flash

PPTP

General Setting

PPTP function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Auth. Type	Pap or Chap		
Data Encryption	Disable		
Encryption Key Length	Auto		
Peer Encryption Mode	Only Stateless		
IP Addresses Assigned to Peer	Start from: 192.168.10.200		
Idle Timeout	0 Min.		

(⚠️ Enable data encryption will use MS-CHAPv2 to authenticate the peer.)

Account Setting

Name	Enable	Type	Peer Network		
BiGuard10	✓	LAN to LAN	192.168.30.100/24	Edit	Delete

[Create](#)

Step4: Click **Save Config** to save all changes to flash memory.

Step5: In another BiGuard as Client, Go to **Configuration > WAN**.

The screenshot shows the WAN configuration page in a web interface. The left sidebar contains a navigation menu with the following items: Status, Quick Start, Configuration, LAN, WAN, Bandwidth Settings, System, Firewall, VPN, QoS, Virtual Server, Advanced, and Save Config to Flash. The main content area is titled 'WAN' and contains the following sections:

- PPTP**
 - Connection Method: PPTP Settings
 - Username: test
 - Password: [masked]
 - Retype Password: [masked]
 - PPTP Client IP: 200 . 200 . 200 . 1
 - PPTP Client IP Netmask: 255 . 255 . 255 . 0
 - PPTP Client IP Gateway: 200 . 200 . 200 . 254
 - PPTP Server IP: 100 . 100 . 100 . 1
 - Connection: Always Connect
 - Idle Time: 10 minutes
 - IP assigned by your ISP: Dynamic (IP automatically assigned by your ISP) Fixed (Your ISP requires you to input IP address)
 - MAC Address: Your ISP requires you to input WAN Ethernet MAC. MAC Address: 00 . 00 . 00 . 00 . 00 . 00
 - DNS: Your ISP requires you to manually setup DNS settings. Primary DNS: 168 . 95 . 192 . 1. Secondary DNS: 168 . 95 . 1 . 1.
 - RIP: Disable. RIP-2B RIP-2M
 - MTU: 1432

At the bottom of the page, there are three buttons: Apply, Reset, and SAVE CONFIG. The Apply button is highlighted in blue.

Step6: Click **Apply**, and **Save CONFIG**.